Evaluation of the Cisco IOS Firewall with DARPA 99 Dataset

Gunes Kayacik, Nur Zincir-Heywood

8th November 2002

Dalhousie University, Faculty of Computer Science, Canada

kayacik@cs.dal.ca, zincir@cs.dal.ca

Abstract

Two open source intrusion detection systems - Snort, Pakemon - and Cisco IOS Firewall with intrusion detection capabilities are benchmarked against DARPA 99 dataset. Performance is characterized using multiple performance metrics. The results show that different tools perform well under different attack categories; hence they can be run at the same time to increase the detection rate of attack instances.

1 Introduction

Security management plays an important role in today's management tasks. Defensive information operations and intrusion detection systems are primarily designed to protect the availability, confidentiality and integrity of critical network information systems. The objective of this work is to compare two open source intrusion detection systems and Cisco IOS firewall to determine the similarities and differences of these systems in terms of detection and to see how these systems can work together. Firewall is used to filter the traffic according to the security policy and intrusion detection systems are deployed to check if there is any intrusion attempts passing through the firewall. Although firewalls and intrusion detection systems carry out different tasks, it is desirable to have a firewall with basic intrusion detection capabilities. This will help administrators to filter some of the intrusion attempts at the firewall level.

The remainder of the paper is organized as follows. Section 2 provides information about Cisco IOS Firewall's intrusion detection features. Test data that is used to evaluate these systems is introduced in section 3. Specifications of the test environment are presented in section 4. Section 5 details the evaluation results of Cisco IOS Firewall, Snort and Pakemon whereas conclusions are drawn in section 6.

2 Cisco IOS Firewall

Cisco IOS is intended to provide a cost effective way to deploy a firewall with intrusion detection capabilities. Cisco IOS Firewall has 59 signatures to detect common attacks and misuse attempts. IDS process sits directly in the packet path and examines packets for intrusion detection. In some cases router may examine the whole packet and maintain the state information for the connection. There are two types of signatures: compound and atomic signatures. For atomic signatures there is no traffic dependent memory requirement because they don't involve connection state. For compound signatures some memory is allocated to inspect the state of the connection[1]. Firewall can be configured to:

- Log the incident
- Drop the packet
- Reset the connection

These signatures are standard for IOS Firewall and they are not updated. These signatures are intended to detect common attacks and probes before the attack. Intrusion Detection is an expensive process in terms of computation time. Since IOS Firewall runs on routers, extensive computations gains more importance. The purpose of the IDS component is to detect basic attacks with minimum CPU time.

3 DARPA 99 Dataset

DARPA 99 dataset provides a standard dataset to evaluate intrusion detection systems. It contains the simulated traffic of a hypothetical military base. Attacks can come from inside or outside. 5 weeks traffic and audit logs are recorded and can be downloaded from [2]. Attacks on DARPA dataset are divided into 5 categories.

1. User to root: Attacker has an account on target machine and tries to use some exploit to get super user access.
2. Remote to Local: Attacker does not have an account on target machine and uses some exploit to get local access.
3. Denial of Service: The objective of the attacker is to prevent legitimate users from using a service.
4. Data: These attacks involve users, who can "technically" perform some action that is not allowed by the security policy.
5. Probe: Before launching an attack it is important to gather information about the target. Probes are intended to gain information that can lead to exploits or attacks.

These categories include many attacks that are listed on MIT site [3].

4 Test Environment

Two Linux machines and two routers are used in evaluation test environment. One Redhat Linux machine is designated as the log machine and a router is configured to send all firewall messages to syslog daemon of this log machine. Another Mandrake Linux machine is used to replay the MIT DARPA99 dataset by using TCPReplay. In the test environment the first router with IDS features examines the packets, sends alerts to syslog server and passes the packets to the second router. Figure 1 shows the basic network diagram of the test environment. All devices are connected with 100Mbps lines.

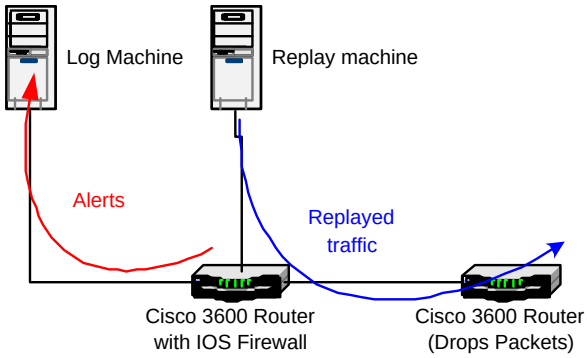

Figure 1 Network diagram of the test environment

The purpose of this research is to evaluate the intrusion detection capabilities of the Cisco IOS firewall. Therefore, no rules are defined to filter or drop any kind of traffic. All 59 signatures and the Content Based Access Control Features are enabled so that FTP, Unix R commands and SMTP sessions are inspected at application level.

5 Evaluation Results

5.1 Cisco IOS

With the intrusion detection alert information, Cisco IOS prints source and destination addresses. Thus, we matched the syslog entries with the attacks on DARPA dataset if and only if the source address in the syslog is equal to the source address in DARPA attack database and the destination address in the syslog is equal to the destination address in DARPA attack database. This corresponds to CL3 confidence level in open source IDS evaluation research[4].

Although there are 59 signatures, only 6 signatures produced alarms throughout the evaluation. Figure 2 shows how many times each signature produced an alarm. Significant number of 3050 signature logs is expected because DARPA dataset contains SYN flood attacks.

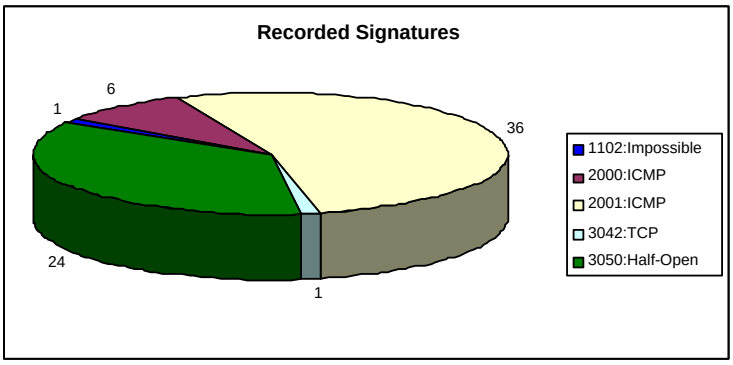

Figure 2 Signatures which triggered the alarms

Signatures

More informations on signatures can be found at [1], whereas the following is a short summary of these signatures.

- **1102 Impossible IP Packet:** This signature is triggered if a packet has same the destination and IP addresses. This signature will catch the land attacks.
- **2000 ICMP Echo Reply:** This signature is triggered if an ICMP message has header the set to 0. (corresponds to echo reply)
- **2001 ICMP Host Unreachable:** This signature is triggered if an ICMP message has header the set to 3. (corresponds to host unreachable)
- **3042 TCP-FIN bit with no ACK in flags:** This signature is triggered if the FIN bit is set and the ACK bit is not set in a TCP packet.
- **3050 Half-open SYN attack / SYN flood:** This signature is triggered if connections are improperly initiated to well-known ports such as FTP, Telnet, HTTP and e-mail.

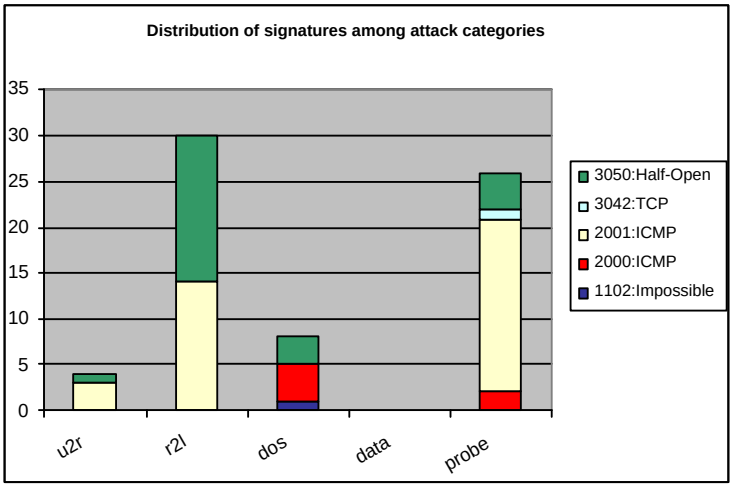

Figure 3. Attacks and signatures that detected the attacks

In figure 3, we see that all of the 1102 signatures are triggered by “land” attack - which is expected - because “land” attack is a denial of service attack. Signature 2001, which produced the majority of the alerts, is distributed among 3 different attack types but it detected most of the probe attacks (which is expected since ICMP messages are used to gather information about a host). Signature 3050 catches half-open connections (namely SYN flood - a DoS attack) so it is difficult to justify why we have signature 3050 on attack categories other than DoS. However, it makes sense to see ICMP signatures falling under probe category since a probe (such as ipsweep) would involve ICMP packets. Since this firewall examines the traffic “briefly” without paying attention to the content, no intrusions under “user to root” (where an attack takes place on the target host) were expected to be detected. However, it may make sense to catch some remote to local attacks since they would start with a probe (which only justifies signature 2000 and 2001).

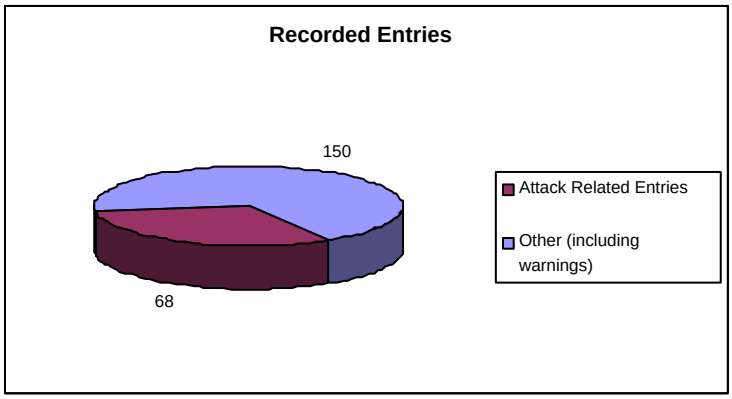

Figure 4. Recorded Entries

As it is shown in figure 4, 31% of the log entries are related with the attacks. Although it is difficult to justify the distribution of signatures among different categories, we can say that Cisco IOS firewall is very precise in logging attacks (compared to the other open source IDS in figure 6).

5.2 Cisco IOS Firewall with other evaluated IDS

Previously, two open source IDS were evaluated with DARPA 99 dataset. In figure 5 we see that Cisco IOS detects less attacks but figure 4 shows that its false alarm rate is much better than the other two intrusion detection systems. As it is shown in figure 6, Cisco IOS has 150 false positives in 218 (~69%) whereas Pakemon has 10603 over 11078 (~95%) and snort has 535231 over 535440 (~99%). We should mention that Cisco IOS firewall enables administrators to turn off the signatures that produces false alarms. Hence, this 69% false alarm rate could be improved (with the expense of false negatives).

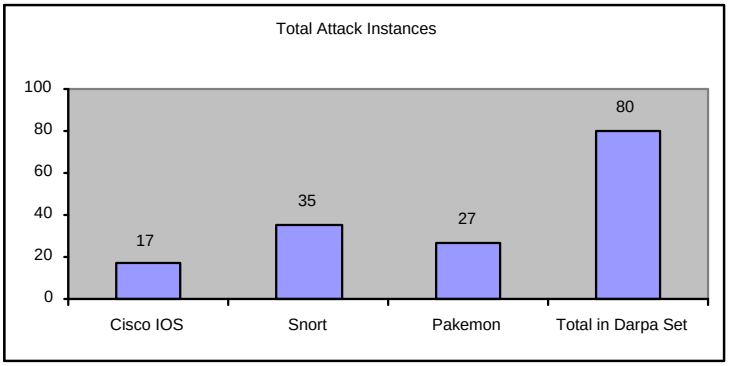

Figure 5. Total detected attacks by each system

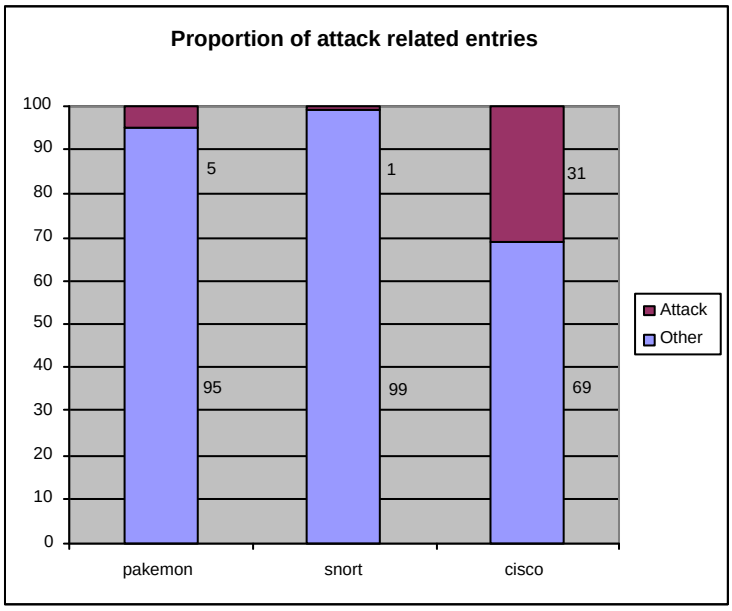

Figure 6. Percentage of attack related entries in logs.

Many of the attacks detected by Cisco firewall were detected by evaluated open source intrusion detection systems as well. This does not make Cisco IOS IDS features less valuable. It examines all the traffic passing through the router whereas open source IDS examines the traffic destined to itself or at most the traffic on the same network segment (i.e. the same hub). Figure 7 details the similarities and differences between three systems in terms of attacks that are detected. Eight attacks, which are detected by all the systems, are listed in table 1:

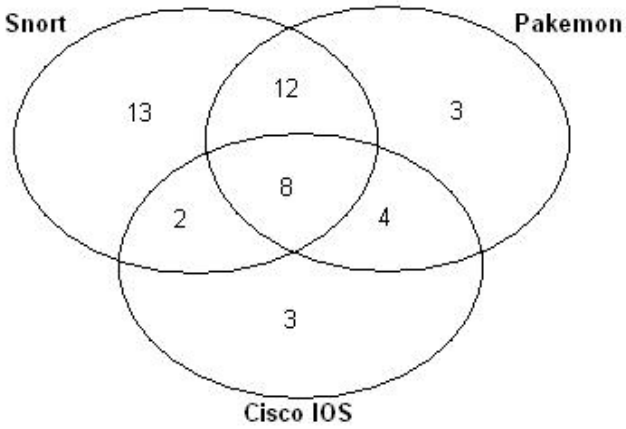

Figure 7. Venn schema of the attacks detected by each system

Attack ID	Attack Name	Attack Type
42.210410	Crash IIS	Denial of Service
43.100000	Power Point Macro	Remote to Local
43.165422	Mail Bomb	Denial of Service
44.091807	ssh Trojan	Remote to Local
44.120500	Power Point Macro	Remote to Local
45.095541	ssh Trojan	Remote to Local
45.114900	Netbus	Remote to Local
45.165009	MS Windows Security Hole	User to Root

Table 1. Attacks detected by the three evaluated systems

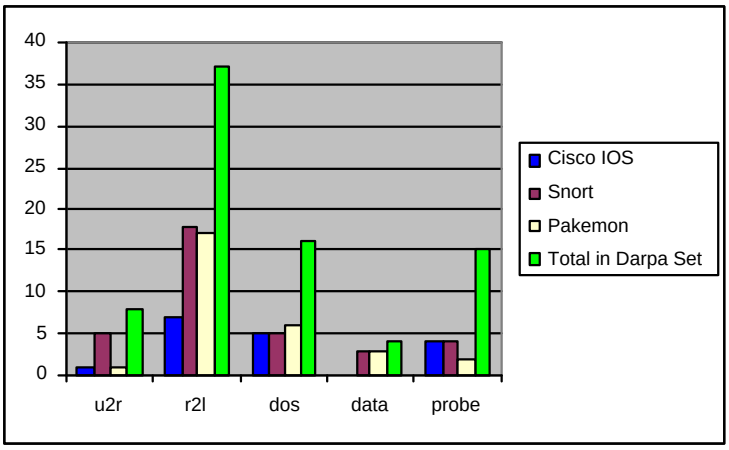

Figure 8. Distribution of detected attacks among different categories.

In figure 8, we can see that Cisco IOS is as good as the other IDS in detecting DoS and Probe attacks.

6 Conclusion

Considering the simplicity of the Cisco IOS' features, this performance is very good, since it does not perform ant complex content inspection. However to detect other categories content inspection is necessary and Snort and Pakemon perform content inspection, which fills this gap.

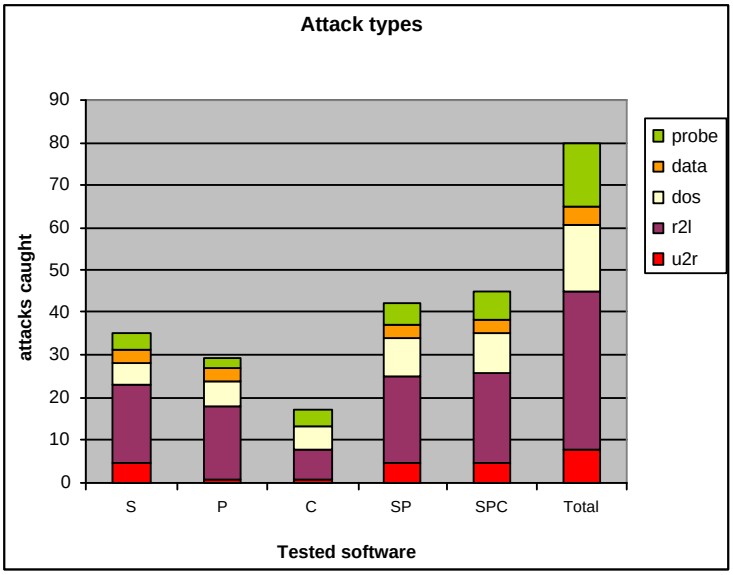

Figure 9. Deployment of intrusion detection systems stand-alone or combined (S: Snort, P:Pakemon, C:Cisco)

Figure 9 shows that by combining two IDSs with Cisco IOS firewall, detected attacks can be increased to 56%.

Acknowledgments

This research was performed in cooperation with Telecom Applications Research Alliance (TARA). We would like to thank Terry Hallett, Bruce MacDougall and Daryl Budden from TARA for their supports in this research as well as Cisco for allowing us to use IOS Firewall in our research.

References

[1] Cisco IOS Firewall Intrusion Detection System, `http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm`

[2] MIT Lincoln Labs. `http://www.ll.mit.edu/IST/ideval/`

[3] DARPA 99 Attack database http://www.ll.mit.edu/IST/ideval/docs/1999/attackDB.html

[4] Kayacik G., Zincir-Heywood A.N., “A Case Study of Three Open Source Security Management Tools”, Technical Report