Intrusion Detection System Using Mobile Agent Technology

Vineet Kumar Chaudhary

Department of Computer Science and Technology, Galgotia College of Engineering & Technology, Knowledge Park-I, Greater NOIDA-201306, Uttar Pradesh, INDIA

Abstract

The Internet and computer networks are exposed to an increasing number of security threats. With new types ofattacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. Intrusions detection systems (IDSs) are systems that try to detect attacks as they occur or after the attacks took place. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. In this context, signature-based network intrusion techniques detection are а valuable technology to protect target systems and networks against malicious activities. Signature-based detection is the most extensively used threat detection technique for (IDSs). One of the foremost challenges for signature-based IDSs is how to keep up

with large volume of incoming traffic when each packet needs to be compared with every signature in the database. When an IDS cannot keep up with the traffic flood, all it can do is to drop packets, therefore, may miss potential attacks. This paper proposes a new model called Signature-based Multi-Layer IDS using mobile agents, which can detect imminent threats with extremely high success rate by dynamically and automatically creating and using small and efficient multiple databases, and at the same time, provide mechanism to update these small signature databases at regular intervals using mobile agents.

Keywords: IDS, intrusion detection systems, mobile agent, signature-based IDS, snort, WEKA Tool, Honeyd

Introduction:

Due to rapid growth of Internet and network based services; security becomes the primary concern for organizations. There are several ways in which an attacker can attack the network of an organization. These can be accessing information for which he is not authorized, bringing down the whole network, etc. The Internet is being used by increasing number of users day by day. A survey [1, 2] show that the number of hosts connected to the Internet has increased to almost 550 million and more than 1.5 billion users are currently using the Internet. The recent survey of Mini Watts Marketing Group [2] estimated that the total number of Internet users was 1,802,330,457 on December 31st 2009. In 2010, the Kaspersky system logged 1,311,156,130 network attacks. That number was just 220 million in 2009. The review [3] shows the major attacks seen in recent years.Review shows that with the

increasing number of Internet users, the cyber crimes also have been increased worldwide to a great value. Fortunately, some intrusion prevention techniques as a first line of defense, such as user authentication (e.g. using passwords and biometrics), avoiding programming errors, and information protection (e.g. encryption) have been applied to protect computer systems.

In the current article we are preparing a security network based on Intrusion Detection System(IDS) [4, 5].We are capturing the packets using packet sniffer tool (Honeyd [6]) and convert those packets in a log file. Weka workbench tool[7]access those log files for association rule mining and convert them in a SNORT [8, 9] compatible format to generate an alarm if any unauthorised intruder wants to access. Mobile agent technology is used through sensors to detect attacks.

Experimental

The experiments were performed choosing two different hardware platforms to simulate attacks and run IDS, one more powerful than the other. The objective was to simulate DDoS attacks on IDSs by running IDS on the slower machine and attacking tools on the faster machine. The aggregate computational and networking resources of attackers usually overwhelm the resources on the IDS machine. In this case, we would like to evaluate the effects of having multiple smaller signature databases and how effectively it helps in improving the throughput and decreasing packet loss rate. A small packet loss rate directly leads to small possibility to miss real attacks that might be hidden in false positive storms. The results should be optimized is our aim.

The detailed hardware and software configurations of systems used for performing experiments are as follows.

Attacking System:

- 2GB memory / Windows 7

- CPU: Intel Core i3 at 2.10 GHz

- 10/100Mbps NIC

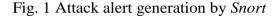
IDS System:

- 4GB memory / UbuntuLinux (based on virtual operating system)

- CPU: Intel Core i3 at 2.10 GHz - 10 Mbps NIC

Attacking Tools: During the period, following tools were used: Demarc SQL Injection, ICMP Destination, DOS UPnP malformed advertisement, PROTOCOL-DNS SPOOF, INDICATOR-SHELLCODE x86 incecx NOOP and INDICATOR-SCAN UPnP Service to trigger alert by the IDS and create a bseline of the most frequent attacks on the network (Fig 1).

M e n u			at			
Curre	ent Ti ue Si	a: 2013-07-27 13:53:03 to 2013-08-10 13:53:04 me: 2013-08-10 13:53:04 gnatures: 7 f Alerts: 1141				
		lert: 2013-08-01 17:28:59 rt: 2013-08-06 16:08:09				
Time	efram	e: 🔻 GO				
Day	:	GO				
Detail by Signatures						
Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	0	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- 0539] [bugtraq 4520]	91	6	8	<u>Summary</u>
1 2		SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002-		6	8 3	<u>Summary</u> <u>Summary</u>
1 2 3	0	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- 0539] [bugtraq 4520]	91	6 1 1	-	
1 2	0 3	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- 0539] [bugtraq 4520] PROTOCOL-ICMP Destination Unreachable Port Unreachable [sid 402]	91 871	6 1 1 2	-	Summary
1 2	0 3 2	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- 0539] [bugtran 4520] PROTOCOL-ICMP Destination Unreachable Port Unreachable [sid 402] DOS UPnP malformed advertisement [sid 1384] PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no	91 871 37	1	-	Summary Summary
1 2	0 3 2	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- (539) [tugitaq 4520] PROTOCOL-ICMP Destination Unreachable Port Unreachable [sid 402] DOS UPnP malformed advertisement [sid 1384] PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority [sid 254]	91 871 37 78	1 1 2	-	Summary Summary Summary
1 2 3 4 5 6 Page	0 3 2 2 1 3 begu	SERVER-WEBAPP Demarc SQL injection attempt [sid 2063] [cve 2002- 0539] [bugtrad 4520] PROTOCOL-ICMP Destination Unreachable Port Unreachable [sid 402] DOS UPnP malformed advertisement [sid 1384] PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority [sid 255] INDICATOR-SHELLCODE x86 inc ecx NOOP [sid 1394]	91 871 37 78 54	1 1 2 3	-	Summary Summary Summary Summary



Analysis of Results

For performing experiment, we considered any attack that appeared at least once as a frequent attack. In addition, all the threats detected in the training period are to be included in the database. Our program scanned all the rule files of Demarc SQL Injection and created a new rule file called "signature.rule" containing the most frequently signatures detected during the training period to be referenced by the snort.conffile as the only signature rule file. In addition, our program created complementary rule files taking out the most frequently used signatures for the

secondary IDS. Demarc SQL Injection was restartedon both systems pointing to the new signature files. To test the performance of all IDS, we conducted ourexperiment using two tests in two different scenarios.In the first scenario, we manually enabled 546packets and attacked the network-using Demarc SQL Injection. In the secondscenario, we let our algorithm do its job by enablingonly the most frequent signatures (in this case 33). Table 1,2 and Figure 2, 3 show the results of our tests in regards of the effects on packet drop rate [10].

Results and Discussion

Our test results clearly show the difference in the performance of the IDS using small signature database comparing to just enabling all signatures. In our environment with our specific configuration, by reducing the size of the database almost 97 times (546/6), on average, we were able to decrease the percentage of the dropped packets by 6.74 times. This is a significant improvement reducing the possibility of a real worm attack sneaking in the midst of dropped packets by the IDS while ensuring all imminent threats can be detected by the IDS. The figure 4 to 7 shows the various steps of the working of network security protocol.

Conclusions

This paper has focused on the efficiency and performance of the new IDS: called signature-based multi- layer IDS using mobile agents. It then discusses the development of a new signature- based ID using mobile agents. The proposed system uses mobile agents to transfer rulebased signatures from large complementary database to small signature database and then regularly update those databases with new signatures detected.

It then describes an experimental setup used to perform the analysis for the verification and validation of proposed SIDS, so that it can be implemented in a large network environment. The results clearly indicate that proposed IDS model performs much better than normal systems with only one database for string signatures. Our experiments proved a significant decrease in the packet drop rate, and as a result, a significant improvement in detecting threats to the network. The paper also highlights the foundations of IDS s and their advantages over other technologies, together with their general operational architecture, and classification provides a for them according to the type of processing related to the behavioural model for the target system. Further, the proposed model can be improved by providing a more comprehensive and automated system that can distribute, add and remove the signatures across databases of multiple IDS systems based on the frequency of their appearance and their level of threat to the network.Finally, we believe more research needs to be done to determine the criteria to choose the optimal training period for a network.

	🖌 🍤 🧲 <default config=""> 😱 🍸 🦉</default>	¥ ▶ ∰• C							
frmMain.java		-						X-	
iource Design	i History 🛛 🕼 😴 🖛 🖉 💐 🖓 🔛 📪 🕴	ê ———							
449	}	Select Netv	vork Adapter:	evice\NPF_{A977E	032-0284-4F97-92A6-1EB5	31DFCE4F}	-	Stop	
450	distinctPages+="NA}";								
451		Device ID:	\D	evice\NPF_{A977E0	032-0284-4F97-92A6-1EB5	31DFCE4F}			
152	wr.write("@ATTRIBUTE sourceip		Blacklisted Ho	sts Breach of Fla	20				
153	wr.write("@ATTRIBUTE destip '		BidCkiisteu Ho	SIS Diedcii Ol Fi	ay				
154	wr.write("@ATTRIBUTE page " ·		urce IP	Source MAC	DestIP	Dest MAC		Protocol	
155	wr.write("@DATA\n");	192.168.1		:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d	HTTP	^	
156	<pre>for (int i = 0; i < dataset.;</pre>			:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d	HTTP		
57	wr.write(dataset.get(i)	+ " <u>192.168.1</u> 192.168.1		:0f:6e:24:6b:03 :0f:6e:24:6b:03	128.83.120.139 128.83.120.139	1c:7e:e5:ab:c4:4d 1c:7e:e5:ab:c4:4d	HTTP		
58	}	192.168.1		:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d 1c:7e:e5:ab:c4:4d	HTTP		
59	wr.close();	192.168.1		:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d	HTTP		
60	<pre>} catch (IOException ex) {</pre>	400 400 4		:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d	HTTP		
61	Logger.getLogger(frmMain.clas	192.168.1		:0f:6e:24:6b:03	128.83.120.139	1c:7e:e5:ab:c4:4d	HTTP		
62	}	192.168.1		:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP		
63		192.168.1		:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP		
64		192,168,1		:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP		
165 L .	}	192,168,1		:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP		
66		192.168.1.	6 4c	:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP		
	<pre>boolean is_present(ArrayList<string></string></pre>		6 4c	:0f:6e:24:6b:03	74.125.236.183	1c:7e:e5:ab:c4:4d	HTTP	-	
468	<pre>for (int i = 0; i < arr.size(); :</pre>								
169	if(arr det(i) eduals(search))								
Dutput									
Debugger Co	onsole × PacketSniffer (run) ×								
Updating ;	property file: C:\jvproj\PacketSniffer\bu	ild							
Compiling	1 source file to C:\jvproj\PacketSniffer'	bu							
Note: C:\	jvproj\PacketSniffer\src\packetsniffer\fm	mMa							
Note: Rec	ompile with -Xlint:deprecation for detail:	s							
	jvproj\PacketSniffer\src\packetsniffer\fr	mMa							
	ompile with -Xlint:unchecked for details.								
compile:		Max. Bandy	vidth: 256	0.0 Kb/s Pa	ackets Transmitted: 34	Save Arff File		38	
run:		Max. Dalla	viuu. 200		ackets fransmitted. 54	Save Amme		50	
Dutput	Q Tasks	_					_		
	•				/	De destGalffes (e	-> 1		IIII 🔂 459/2
_						PacketSniffer (n	un)	running	
A DECKER OF			4					Desktop ²⁰ EN	▲ 🕅 📲 🕺

Fig. 4 Packet capturing by Honeyd

📝 C:\jvp	projPacketSniffe/outputarff - Notepad++
<u>Eile E</u>	dit <u>S</u> earch <u>V</u> iew Encoding <u>L</u> anguage Settings Macro Run Plugins <u>Wi</u> ndow <u>?</u>
Ø	'< 1 ● 1 ● 1 ● 1 ● 1 ● 1 ● 1 ● 1 ● 1 ● 1
🔚 ot	utput.arff
1	 Title: Packet Captured
2	%2. Author: Vineet
3	@RELATION packets
4	@ATTRIBUTE sourceip {192.168.1.6,0.0.0.0}
5	<pre>@ATTRIBUTE destip {130.217.208.182,173.194.36.97,74.125.236.183,128.83.120.139,0.0.0.0}</pre>
6	@ATTRIBUTE page {"www.cs.waikato.ac.nz/ml/weka/index.html HTTP/1.1","www.google-analytics.com/ utm.gif","www.cs.waikato.ac.nz/ml/publications.html HTTP/1.1","www
7	@DATA
8	192.168.1.6,130.217.208.182,"www.cs.waikato.ac.nz/ml/weka/index.html HTTP/1.1"
9	192.168.1.6,173.194.36.97, "www.google-analytics.com/ utm.gif"
10	192.168.1.6,173.194.36.97, "www.google-analytics.com/ utm.gif"
11	192.168.1.6,130.217.208.182, "www.cs.waikato.ac.nz/ml/publications.html HTTP/1.1"
12	192.168.1.6,130.217.208.182,"www.cs.waikato.ac.nz/ml/main.css HTTP/1.1"
13	192.168.1.6,130.217.208.182, "www.cs.waikato.ac.nz/ml/publications top.html HTTP/1.1"
14	192.168.1.6,130.217.208.182, "www.cs.waikato.ac.nz/ml/publications menu.html HTTF/1.1"
	192.168.1.6,130.217.208.182, "WWW.cs.waikato.ac.nz/ml/publications2012.html HTTP/1.1"
16	192.168.1.6,130.217.208.182, "WWW.cs.waikato.ac.nz/ml/favicon.ico HTTF/1.1"
17	192.168.1.6,173.194.36.97."www.google-analytics.com/ utm.gif"
18	192.168.1.6,173.194.36.97, "www.google-analytics.com/ utm.gif"
19	192.168.1.6,74.125.236.183, "www.google.co.in/xjs/ /ja/k=xjs.s.en US.jOYpRJj4zMA.O/m=sy5,cdos,gf,vm,sy64,sy66,sy65,sy150,tbui,mb,sy68,sy69,sy71,sy73,sy70,sy74,sy11
	192.168.1.6,74.125.236.183,"www.google.co.in/gen 204"
	192.168.1.6,74.125.236.183,"www.google.co.in/gen 204"
22	192.168.1.6,74.125.236.183,"www.google.co.in/url"
23	192,168,1.6,128,83,120,139, "WWW.cs.utexas.edu/users/ml/tutorials/Weka-tut/ HTTP/1,1"
24	192.168.1.6,128.83.120.139. "www.cs.utexas.edu/favicon.ico HITP/1.1"
25	192.168.1.6,128.83.120.139,"www.cs.utexas.edu/users/ml/tutorials/Weka-tut/sld004.htm HTTP/1.1"
26	192.168.1.6,128.83.120.139,"www.cs.utexas.edu/users/ml/tutorials/Weka-tut/first.gif HTTP/1.1"
27	192.168.1.6.128.83.120.139. "www.cs.utexas.edu/users/ml/tutorials/Weka-tut/prev.gif HTTP/1.1"
28	192.168.1.6,128.83.120.139, "www.cs.utexas.edu/users/ml/tutorials/Weka-tut/next.gif HTTP/1.1"
	192.168.1.6,128.83.120.139,"www.cs.utexas.edu/users/ml/tutorials/Weka-tut/last.gif HTTP/1.1"
	192.168.1.6,128.83.120.139,"www.cs.utexas.edu/users/ml/tutorials/Weka-tut/space.gif HTTP/1.1"
	192.168.1.6,128.83.120.139, "www.cs.utexas.edu/users/ml/tutorials/Weka-tut/info.gif HTTP/1.1"
32	192.168.1.6.128.83.120.139."www.cs.utexas.edu/users/ml/tutorials/Weka-tut/text.oif HTTP/1.1"
< [
lormal t	text file length : 5053 lines : 42 Ln : 6 Col : 913 Sel : 0 UNIX ANSI UVS
🔊	📔 💿 🥹 🗊 🖾 💽 💰 🚿

Fig. 5 arff output file

🖉 Weka GUI Chooser 📃 📃	😨 Weka Explorer	- • ×
Program Visualization Tools Help	Preprocess Classify Cluster Associate Select attributes Visualize	eka+data+mining+tutorial&n 😭 😰 🔳
The University of Waikato	Open file Open DB Generate Undo Edit Save Filter Choose Apply Open tellion Apply	SIGN IN
Waikato Environment for Knowledge Analysis Kno Version 3.6.9		\$
(c) 1999-2013 The University of Wakato Hamilton, New Zakaho University of University o	Attributes No. Label Count All None Invert Pattern 1 192.168.1.6 34 No. Name None 0 0 0 1 sourcep 2 destp 0 0	
2 %2. Author: Vinet 3 @RLATION packets 4 @ATTRIBUTE destip [130. 6 @ATTRIBUTE destip [130. 6 @ATTRIBUTE page ("www.c 7 @DATA 8 192.168.1.6,130.217.208 9 192.168.1.6,173.194.36. 10 192.168.1.6,173.194.36. 11 192.168.1.6,130.217.208 4 192.168.1.6,130.217.208 12 192.168.1.6,130.217.208 4 192.168.1.6,130.208		
Data mining with W www.lbm.com/develop Apr 27, 2010 - Data mit load data into WEKA, w with IBM's products, as Introduction - What is da	ing is a collective term for dozens of techniques to glean To have to put it into a format that will be understood them well as our most popular articles and tutorials. ta mining? - WEKA - Regression	I
Weka Video Tutori	als :: Data Mining, Text Mining, neural network	
📀 📋 🔽 🔮 🚺		Desktop ^{**} EN 18:14 07/30/2013

Fig.6 Pre processing in WEKA Tool

Veka Explorer		
	Cluster Associate Select attributes Visualize	
ociator		
Choose Apriori	I-N10-T0-C0.9-D0.05-U1.0-M0.1-5-1.0-c-1	
tart Stop	Associator output page	
ult list (right-click		
uit list (right-click 14:23 - Apriori		
eneo Apriori		
	Apriori	
	Minimum support: 0.1 (3 instances)	
	Minimum metric <confidence>: 0.9</confidence>	
	Number of cycles performed: 18	
	Generated sets of large itemsets:	
	Size of set of large itemsets L(1): 8	
	Size of set of large itemsets L(2): 10	
	Size of set of large itemsets L(3): 3	
	Size of set of large itemsets L(3): 3	
	Best rules found:	
	1. destip=128.83.120.139 13 ==> sourceip=192.168.1.6 13 conf:(1)	
	<pre>2. destip=74.125.236.183 10 ==> sourceip=192.168.1.6 10</pre>	
	4. page=www.google.co.in/gen 204 7 ==> sourcej=192.168.1.67 conf:(1)	
	5. page=www.google.co.in/gen_204 7 ==> destip=74.125.236.183 7 conf:(1)	
	6. destip=74.125.236.183 page=www.google.co.in/gen_204 7 ==> sourceip=192.168.1.6 7 conf:(1)	
	7. sourceip=192.168.1.6 page=www.google.co.in/gen_204 7 ==> destip=74.125.236.183 7 conf:(1)	
	<pre>8. page=www.google.co.in/gen_204 7 ==> sourceip=192.168.1.6 destip=74.125.236.183 7 conf: (1) 9. destip=173.194.36.97 4 ==> sourceip=192.168.1.6 4 conf: (1)</pre>	
	10. page=www.google-analytics.com/ utm.gif 4 ==> sourceip=192.168.1.6 4 conf:(1)	
JS		
		Log

Fig. 7 Association rule mining in WEKA Tool

References

- Internet System Consortium, "ISC Domain Survey: Number of Internet Hosts." http://ftp.isc.org/www/survey/repor ts/2010/04/. Last updated: May 12, 2010.
- Internet World Stats, "Internet User Statistics – The Internet Big Picture: World Internet Users and Population Stats." http://www.internetworldstats.com/ stats.htm. Last updated: May 3, 2010.
- [3] R.Miller, "Twitter is Latest Victim in Series of Attacks." Internet: http://www.datacenterknowledge.c om/archives/2009/08/06/twitter-islatest-victim-in-series-of-attacks/. Last updated: Aug 6, 2009.
- [4] R. G. Bace, *Intrusion detection: Sams*, 2000.
- [5] R. Base and P. Mell, *Intrusion Detection Systems*, National Institute of Standards and Technology (NIST), Special Publication, vol. 51, pp. 800-831, 2001.

- [6] D. Dagon, X. Qin, G. Gu, W. Lee,
 J. Grizzard, J.Levine, and H.
 Owen, "Honeystat: Local wormdetection using honeypots," *RAID 2004*, LNCS 3224,pp. 39-58, 2004.
- [7] Ian H. Witten; Eibe Frank, Mark A.
 Hall (2011). "Data Mining: Practical machine learning tools and techniques, 3rd Edition".
 Morgan Kaufmann, San Francisco.
 Retrieved 2011-01-19.
- [8] D. Bailey, Sneeze.
 (http://archives.neohapsis.com/arch
 ives/snort/2001-08/0180.html)
- [9] J. Beale, A. R. Baker, B. Caswell, and M. Poor, Snort 2.1 Intrusion Detection: Syngress Media Inc, 2004.
- [10] B. C. S. Ryu and J Kim, "design of packet detection system for highspeed network environment," in *The6th International Conference Advanced Communication Technology*, pp. 496-498, 2004.