Key Benefits

Honeypot based intrusion detection

Real time detection

Detects unknown threats

Effective against internal and external threats

Simple to use

Highly configurable

Advanced server emulation

Detailed logging

No false positives

Lower hardware

Lower total cost of ownership

Product Overview

New threats are constantly emerging to the security of organisations' information systems infrastructure. Firewalls and VPNs cannot prevent all intrusions and do little to prevent attacks from within the organisation itself.

Intrusion detection plays a vital role in ensuring the integrity of a network's security. Network intrusion detection systems (NIDS) have long been seen as the most effective means of detecting attacks. However they do have significant weaknesses.

The increasing quantity and diversity of legitimate network traffic has resulted in ever increasing hardware costs and the large number of false positive alerts generated can be too much to analyse effectively.

By relying on the search for known attack signatures NIDS are unable to detect new forms of attacks and the use of encryption prevents them examining traffic altogether.

An additional approach is required to tackle such problems.

Honeypot technology

A honeypot is a system that is put on a network with the intention that it can be probed and attacked, in order to gain information on an attacker. This concept is a radically different approach to other forms of security and one that is increasingly being recognised to be very effective in detecting security threats.

INTERNET

FSenso

By allowing intruders to interact with the honeypot, detailed

information can be gathered on the techniques and tools that they use. Because there is no legitimate use for the honeypot, all connections it receives are suspect. This results in very few false positive alerts.

KFSensor has been developed from the ground up, as a production honeypot system, dedicated to the task of intrusion detection. Used as part of a comprehensive security strategy, KFSensor adds an additional layer of protection to detect security breaches that may not be picked up by other means.

	View Scenario Settings Help								
1	🗏 😸 😹 💽 🕹 🕴	Ş 🕻	1 7 6	ei 屋 🛠					
3	127.0.0.1 - Main Scenario		ID	Start Time	Pr	Sens	Name	Visitor	Received
ė.	CP TCP		4365	20:59:07.125	TCP	5900	VINC	pc1-mapp2-6-cust64	RFB 003.003[0A]'tm[
	🐗 21 FTP Guild - Recent A	۱c	4364	20:39:45.562	UDP	1434	MS SQL Server	1Cust68.tnt42.mia5.d	[04 01 01 01 01 01 01 0
		Ξ	OP 4363	20:36:59.234	TCP	80	IIS	IS~NEGAHDARI2	GET /default.ida?XXX
	a 23 Telnet		() 4362	19:53:52.421	TCP	25	SMTP	211.201.15.8	HELO 45×gl9b3rsi78s
			OP 4361	19:05:55.625	TCP	1080	WinGate	www.vipondassociate	[05 01 00]
	🚭 🚭 25 SMTP - Recent Activ	vi	OP 4360	19:05:53.031	TCP	1080	WinGate	www.vipondassociate	[04 01 01 A4 D1 A4 1
			4359	18:12:35.281	TCP	21	FTP Guild	p508E3E58.dip.t-diali	USER anonymous[0D
	🛛 🕌 80 IIS - Recent Activit	y	O 4358	16:02:53.343	TCP	17300	Kuang 2, Trojan	12-230-64-180.client	
	4 110 POP3		4357	15:58:17.187	UDP	111	sunrpc	61.185.147.2	g[00]\$[A6 00 00 00 0
	🐳 111 sunrpc		9 4356	15:15:01.015	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%252f
	4 113 ident		4355	15:15:00.828	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%25%
			Q 4354	15:15:00.593	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%%35
	🐗 143 imap		Q 4353	15:15:00.375	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%%35
			Q 4352	15:15:00.140	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%c1%
			Q 4351	15:14:59.921	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%c0%
	🚽 🕼 1024 NetSpy, Trojan			15:14:59.671	TCP	80	IIS	VICENTE-PL4D3RX	GET /scripts/%c0%
	4 1080 WinGate - Recen	F	¥ 1010	15:14:59.437	TCP TCP	80 80	IIS	VICENTE-PL4D3RX	GET /scripts/%c1%
	1214 Grokster, P2P file sha		0 4348 0 4347	15:14:59.250 15:14:59.062	TCP	80	IIS	VICENTE-PL4D3RX VICENTE-PL4D3RX	GET /msadc/%255c
				15:14:59.062	TCP	80	IIS	VICENTE-PL4D3RX VICENTE-PL4D3RX	GET /_mem_bin/%2
1	433 MS SQL Server	×	-	10:14:08.795	TOP		115	VICENTE-PL4D3RX	GET /_vti_bin/%25
<		> j	<			111			i i
leac	dy								NUM

How KFSensor works

KFSensor is easy to install and configure. It takes just five minutes to set up and become operational. No special hardware is required and its efficient design enables it to run even on low specification Windows machines.

Its straightforward Windows interface controls all functionality. There is no need to edit complex configuration files and it comes pre-

Key **Focus**

configured with all the major systems services required.

KFSensor works by simulating systems services at the highest level of the OSI Network Model - the application layer. This enables it to make full use of Windows security mechanisms and networks libraries, reducing the risk of detection and compromise by not introducing additional drivers and custom IP stacks. A machine running KFSensor can be treated as just another server on the network, without the need to make complex changes to routers and firewalls.

KFSensor provides immediate benefits in revealing the nature and quantity of attacks on a network. By consolidating all the network traffic of an attack into a single alert KFSensor makes it easy to explain a security threat to non-specialist staff.

The information KFSensor generates can be used to refine firewall rules and produce new signatures for network intrusion detection systems.

KFSensor is an extremely cost effective way of enhancing network security infrastructure.

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource" - The Honeypot Maillist Group



Key Features

Production honeypot Monitors multiple ports All ports configurable Define custom responses Supports both TCP and UDP services

Sophisticated emulation of system services including:

- FTP
- \cdot HTTP
- POP3
- · Telnet
- SMTP
- VNC

Sanda alarta hy amail

DOS attack protection

All bytes of attack are logged

System tray indicator

Colour coded alert warnings

Filter logs by port or IP address

Configurable reports

Export logs in multiple formats

For more information on KFSensor look at our website:

www.keyfocus.net

or email us at

contact@keyfocus.net

Product Features

At the heart of KFSensor sits a powerful internet daemon service that is built to handle multiple ports and IP addresses. It is written to resist denial of service and buffer overflow attacks.

FSenso

Building on this flexibility KFSensor can respond to connections in a variety of ways, from simple port listening and basic services (such as echo), to complex simulations of standard system services. For the HTTP protocol KFSensor accurately simulates the way Microsoft's web server (IIS) responds to both valid and invalid requests. As well as being able to host a website it also handles complexities such as range requests and client side cache negotiations. This makes it extremely difficult for an attacker to fingerprint, or identify KFSensor as a honeypot.

Every byte of an attack is recorded in KFSensor's logs. Events can be assigned different colour coded severities, making it easy to spot anything unusual or serious. Custom reports can be defined and the log can be filtered to show just those from a certain port, protocol or source IP address.

File View Scenario Settir	ngs Help										Event Detail	s				2
1 2 3 4 🗶	it it 🔍	📴 🏋 🖨 Ai 🔟	\$						Event Start Time:	15/06/2003 19:53:52.421 Event ID: 43			4362	62		
2 127.0.0.1 - Main Scenario			ID	1 9	Start T	ime	Pr	Sens	Name		End Time:	15/06/2003 19:54	:04.781	Туре:	Connection	
					0:59:0	07.125	TCP	5900	VNC		Description:	11				
				54 2	0:39:4	:39:45.562 UDP 143	1434	I MS SQL Serve	ver	Severity:	: High					
61.185.147.2 - Activity			9 436		20:36:5		80	IIS								
60 120 240 60 1 Cush60 kak42 asiaE da uu aab Dar						52.421	TCP	25	SMTP		Visitor IP:	211.201.15.8 Port: 1057				
			9 436		9:05:5	55.625	TCP	1080	WinGate		Domain:					
			9 4360		DOS	DOS Attack Settings			X							
<u> </u>	-		9 4359 6 1358		Lin	Limits					Sensor Name:	SMTP				
- 🧏 209.164.40.228 - 👔	dit Sim Std Server - HTTP				Ma	Max Clients:			50 bjar							
	Title		43) _{Me}	ax Receive Si	ze (Bytes):		10240		IP:	217.39.120.63	Port:	25		
213.37.192.47 - VI	Name:	IIS	43		1						Bound:		Protocol:	TCP		
	Description:	IIS Sm	43		Ma	ax Receive Lo	ig Size (By	tes):	1024		Action:	SimStdServer	Sim Server:	SMTP		
🙎 217.219.65.11 - I	Default Port: 80 Severity: High 🗸			53 1	Visitor DOS Attack Limits						Details					
	Options Emulation:		439		Ma	ax Concurren	t Connecti	ons Per IP:	20		Closed By:	Server	Limit Excee	ded:		
		Microsoft IIS 6.0 ¥	435		Ma	Max Connections Per IP	100		Received:							
	Version: Microsoft-IIS/6.0			50 1		Lock Out For (Minutes):		1440		HELO 45xgl9b3rsi78s					Expand	
Document Root: files/js/ywwroot Index Files: isstart.htm Default.htm index.htm index.html		4349						1110			:OM: <cool@mail.co.kr> D: <cool@mail.co.kr></cool@mail.co.kr></cool@mail.co.kr>					
				(Global DOS Attack Limits			1000		DATA						
	Time out:	20 (Seconds)	434		1	ax TCP Conne										
	Receive Limit:	10240 (bytes)	434	1 6 1	e Ma	ax UDP Conn	ections:		1000		Response:					
	Log response lines:	(4) (11)			Re	eset Lock Up	After (Hou	rs):	6		HELO 45x0	i networksforu.com M gl9b3rsi78s i networksforu.com H			rvice, V 🛕	Expand
ady Log response size: 1024 (bytes)								ок	Cancel		MAIL FROM	M: <cool@mail.co.kr< td=""><td>></td><td>12:0]</td><td>~</td><td></td></cool@mail.co.kr<>	>	12:0]	~	
	Log receive size:	500 (bytes)			1						<	111			>	
		OK Cancel Help					D	efault	Help			Next	Previous	Close		telp

Example SMTP attack and response

By emulating the behaviour of a vulnerable SMTP server an attacker uses it in an attempt to relay spam. This reveals the source and purpose of the attack with no risk of compromise.

>>>>220 networksforu.com Microsoft ESMTP MAIL Service, Version: 6.0.2600.1106 ready at Mon, 10 Jun 2003 17:26:21 +0000 HELO qqq-6j4vecjhtdb >>>>250 networksforu.com Hello [61.99.243.194] MAIL FROM:<SuperMan2173912016@hotmail.com> >>>>250 2.1.0 SuperMan2173912016@hotmail.com....Sender OK RCPT TO:<ch69v5@hotmail.com> >>>>250 2.1.5 ch69v5@hotmail.com DATA >>>>354 Start mail input; end with <CRLF>.<CRLF> From: <SuperMan2173912016@hotmail.com> To: ch69v5@hotmail.com Subject: SuperMan - 217.39.120.16 X-Mailer: SuperMail v1.1 Mime-Version: 1.0 Content-Type: text/plain;%09charset=us-ascii Server Test - 217.39.120.16 >>>>250 2.6.0 <NETWORKSFORULvx4efKx00008432@networksforu.com> Queued mail for delivery OUIT

About KeyFocus

Keyfocus is a software company dedicated to developing network and system security software. KeyFocus was one of the first companies to recognise the potential of honeypot technology to move beyond a research tool and become a valuable production system, which could complement and enhance an organisation's existing security infrastructure.

Our goal is to work closely with our customers so we can continue to offer the best product in this exciting and rapidly developing field.