Visual Support for Analyzing Network Traffic and Intrusion Detection Events using TreeMap and Graph Representations

Florian Mansmann¹ Fabian Fischer¹ Daniel A. Keim¹ Stephen C. North²

¹ University of Konstanz, Germany ² AT&T Research, Florham Park, NJ, U.S.A.

Symposium on Computer-Human Interaction for Management of Information Technology, Baltimore, MD, 2009



Introduction



Photo by Guillaume Paumier / Wikimedia Commons, CC-by-sa-3.0



Introduction



Photo by Guillaume Paumier / Wikimedia Commons, CC-by-sa-3.0



How to combine all the data?

Intrusion Detection e.g. Generated IDS Events, Firewall Logs Network Traffic e.g. NetFlow connections, Bandwidth data,...



Visual Analytics with NFlowVis





🛓 NFlowVis

File Tools Export Data Help



Daily Traffic Overview



Daily Traffic Overview (Flows per Minute Widget)

🚣 NFlowVis

File Tools Export Data Help

NElowVic	1. Overview 2. Intrusion Detection View 3a. Flow Visualization 3b. Graph 4. Host Details 5. NetFlow Records	
NetFlow Visualization Tool	IDS Data Source	
	<query template=""></query>	
	Suspicious Hosts Template Settings	
Project Selection Attribute Value Flows 108.142.800 Start Time 2008-04-01 23:5 End Time 2008-04-03 00:0 Packets 2.007.256.358 Payload 1.238,35 GiB Source IP 2.877.353 Destination IP 2.890.423 Ok dstaddr Max OK dstaddr OK Metwork Tools	<query template=""> Suspicious Hosts Refresh Host List</query>	× .
	Visual Connection Analysis Ignore single flow connections I Include any traffic between hosts	

Intrusion Detection View

🚣 NFlowVis

File Tools Export Data Help

NFlowVis	1. Overview 2. Intrusion Detection View 3a. Flow Visualization 3b. Graph 4. Host Details 5. NetFlow Records
NotElow Vigualization Tool	IDE Data Equipo
Netriow visualization room	
	<query template=""></query>
	<query template=""></query>
Project Selection	Aggregated SNORT IDS Alerts
Project Selection	Brute Scan Attacker (SSH)
2008-04-02	Communication with Blacklisted Hosts (DShield)
Attributo Voluo	Communication with Blacklisted Hosts
Flows 109 142 900	DBVIS
Start Time 2008-04-01 22:5	Distributed Brute Scan Attacker (SSH)
End Time 2008-04-03 00:0	Julegai SMIP Servers
Packets 2.007.256.358	
Pavload 1,238,35 GiB	
Source IP 2.877.353	
Destination IP 2.890.423	
Quick Lookup	
srcaddr -> dstaddr	
OK	
dstaddr 🔻 🗖 Raw Records	
ОК	
Network Tools	
WHOIS	
ОК	
	Visual Connection Analysis Ignore single flow connections Include any traffic between hosts

- 🗆 🗡

Intrusion Detection View – Select IDS Data Source

🕌 NFlowVis

File Tools Export Data Help

	I. Overview 2. Indus	ion Detection View 3a.	. Flow Visualization 3	b. Graph 4. Host Det	ails 5. NetFlow Rec	ords		
triow Visualization Tool	IDS Data Source							
	Aggregated SNORT I	DS Alerts						
	Suspicious Hosts Te	emplate Settings						
2008-04-02	Refresh Host Lis	it _						
All the Market	srcaddr	msg	typesofalert	alerts 🗸	count	hostcount	dpkts	doctets
Attribute Value	134.34.53.42	ICMP Echo Reply,	4	172.917	8.197	8	88.135	62.855.538
10ws 108.142.800	85.131.189.69	ICMP PING, ICMP	3	141.552	2.022	6	40.745	3.307.236
tart Time 2008-04-01 23:5	134.34.53.254	ICMP IRDP router	3	91.437	2	2	579	48.636
nd Time 2008-04-03 00:0	134.34.53.228	DDOS - TFN dient	10	79.362	2	2	13	1.035
ackets 2.007.256.358	134.34.53.47	ICMP Echo Reply,	6	27.735	495	8	3.150	344.316
ayload 1.238,35 GB	134.34.53.135	(http_inspect) BA	3	21.566	3.648	9	31.571	3.086.333
ource IP 2.877.353	134.34.53.94	(http_inspect) BA	5	21.150	272	6	11.848	753.438
estination IP 2.890.423	134.34.53.72	MISC UPnP malfor	4	12.667	235	7	21.257	1.787.190
	134.34.53.115	ICMP PING, ICMP	6	8.224	843	7	2.485	166.479
ick Lookup	134.34.3.34	ICMP PING, ICMP	3	6.250	3.160	523	1.780.706	278.255.45
ckeokup	134.34.20.4	ICMP PING	1	5.986	25.024	11.954	576.235	169.466.28
caddr -> dstaddr 🔹	134.34.53.73	ICMP L3retriever	9	3.559	53	4	154	16.47
101 100 00	91.23.178.176	ICMP PING, ICMP	2	2.702	1	1	1	7
5.131.189.69	134.34.3.26	ICMP PING, ICMP	3	2.247	3.922	534	2.681.391	567,543,10
ок	134.34.53.200	SHELLCODE x86	3	1.487	112	2	177	13.26
	134.34.3.24	ICMP PING.ICMP	3	1.355	3.607	531	2.575.695	380.845.86
staddr 🔻 🗖 Raw Records	134.34.53.160	ICMP PING, ICMP	4	1.067	1.159	7	9,183	6.812.82
	134.34.53.222	SNMP public acces	2	854	39	8	2.234	273.82
5.131.189.69 OK	134.34.57.166	ICMP Echo Reply	2	848	2,425	10	326.050	120.961.78
	134.34.53.133	ICMP L3retriever	5	819	565	4	782	74.13
and Table	134.34.53.223	ICMP L3retriever	2	813	654	9	12,162	2.761.59
WORK TOOIS	134.34.53.41	SCAN UPnP servic	3	771	46	11	21.525	14,299,90
HOIS 👻	134.34.53.159	SNMP public acces	2	654	104	9	2,998	309.42
	134.34.53.148	ICMP L3retriever	4	393	25	8	1.789	208.63
5.131.189.69 OK	134.34.53.19	ICMP L3retriever	4	213	5	4	552	115.29
	134.34.53.20	ICMP PING.MISC		164	53	5	2.078	173.30
	134,34,53,150	ICMP L3retriever	4	158	7	4	97	10.39
	206,222,25,144	ICMP PING	1	152		1	554	25.48
		ICMD I Protriever		143	54	7	5,526	692.20

Intrusion Detection View – Suspicious Hosts

🛓 NFlowVis

File Tools Export Data Help

Project Selecton Dis Data Source Project Selecton Project Selecton Carda Selecton Selecton Carda Selecton Carda Selecton Selec	NetFlow Visualization Tool	IDS Data Source Aggregated SNORT ID Suspicious Hosts	S Alerts mplate Settings						
Project Sclection Supriorited Sclecting Supriorited Sclecting 2008-04-02 ▼ Attribute Yake Power 108,142,800 Start Time 2008-04-02 Packet 2009-04-02 Start Time 2008-04-01 Packet 2007-255,538 Packet 2007-255,538 Packet 2007-255,350 Packet 2007-255,350 Packet 2007-255,350 Pethodson 3 2.247 3.922 534 2.661.391 575.655 300.454.683 Source IP 2.890.423 1004 PNNG(LOP 3 1.325 3.607 531 2.257.655 300.454.683 Source IP 2.890.423 1004 PNNG(LOP 3 1.343.33.31 1004 PNNG(LOP 3 4.326 100 300.246 <t< td=""><th></th><td>Aggregated SNORT ID Suspicious Hosts Ter</td><td>S Alerts mplate Settings</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>		Aggregated SNORT ID Suspicious Hosts Ter	S Alerts mplate Settings						
Unit Suspice Suspice 2008 04 02 Attribute Suspice		Suspicious Hosts Ter	mplate Settings						T
Project Selection Refease Host List Power 00:442.00 Start Time 200:442.00 Start Time 200:442.00 Start Time 200:442.00 Start Time 200:42.00 Start Time 200:42.00 Start Time 200:42.00 Start Time 200:42.00 Start Time 200:7255.358 Packets 2007:255.358 Packets 2007:255.358 Packets 2007:255.358 Packets 200:42.00 Start Time 200:42.00 Start Time 200:42.00 Start Time 200:42.00 Start Start 200:42.00 St			inplate setungs j						
Refeat Host List Construction Value Flows 103.142.800 CMP Destination 1 2 278.642 1.622 37.215.363 5.364,153.538 A Start Time 2008-04-03 000 1 2 278.642 1.623 37.215.363 5.364,153.538 A Packets 2007 275.63.987 2007 275.63.987 2007 275.63.987 2007 275.63.987 2007 275.63.182 109.166 3.642 37.215.363 5.364,153.538 A Destination IP 2.807 23.66 3.667 3.668 9 31.571 3.3668.333 13.343.3.24 CUMP PDIG (CMP	Project Selection		· · · ·						
2030+02 Image: standard standard <thstandard< th=""> standard</thstandard<>	2000.04.02	Refresh Host List							
Value value srcaddr mg typesofaett count Postcount dpkts doctets Flowis 108,142.80 200-04-0123.s 1 5.996 2.20,24 11.93 5.7235 139.453.53.8 A Packets 2000-04-0123.s 1 1.23,35.56 139.453.53.8 199.4652.538 199.4652.538 199.4652.538 199.455.538 199.455.538 199.455.538 199.455.538 199.455.538 199.455.538 199.455.558 <th>2008-04-02</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	2008-04-02								
Image: 1008 1008 <th>Attribute Value</th> <td>srcaddr</td> <td>msg</td> <td>typesofalert</td> <td>alerts</td> <td>count 🗸</td> <td>hostcount</td> <td>dpkts</td> <td>doctets</td>	Attribute Value	srcaddr	msg	typesofalert	alerts	count 🗸	hostcount	dpkts	doctets
Start Time 2008-04-01 225 103-34.20.4 ICVP PINS 113-34.32.0 103-34.25.12 103-34.25.12 103-34.25.12 103-34.25.12 103-34.25.12 103-34.25.12 103-34.25.12 103-34.55.13 103-34.55.10 103-34.55.13 1	Flows 108.142.800	134.34.3.28	ICMP Destination	1	2	278.642	1.823	37.215.369	5.364.153.538
Packet b 2008-04-03 00:0 4 172-317 8.197 8 88.135 62.855.538 Packet b 2.007.256.338 123.33.5 GB 5007.256.338 9 31.571 30.66.333 Destination IP 2.890.423 123.33.5 GB 134.34.3.24 ICMP PING.ICMP 3 6.250 31.160 523 1.775.695 300.8458.643 Destination IP 2.890.423 ICMP PING.ICMP 3 6.250 3.165 5.007 73.389 4.404.492 I34.34.3.7.166 ICMP PING.ICMP 3 6.250 3.160 523 1.780.7669 279.255.455 I34.34.53.119 ICMP PING.ICMP 3 6.250 3.100 73.389 4.404.492 I34.34.53.119 ICMP PING.ICMP 3 6.149.52 2.002 73.389 4.404.492 I34.34.53.119 ICMP PING.ICMP 3 14.1552 2.002 6 49.7745 33.071.766 13.377.266 13.377.266 13.33.751 33.22 33.299 30.619.596 13.43.53.190 ICMP PING.ICMP 3 14.1552 2.002 6 4.7745 33.072	Start Time 2008-04-01 23:5	134.34.20.4	ICMP PING	1	5.986	25.024	11.954	576.235	169.466.288
Packets 2.007.256.358 Payload 2.247 3.922 534 2.681.391 567.543.102 Payload 1.233.35 GB 1.233.35 GB 321.556 3.648 9 31.575 3.006.333 Destination IP 2.890.423 134.343.3.14 ICMP PING/ICMP 3 1.555 3.607 531 2.575.695 380.845.643 134.34.3.34 ICMP PING/ICMP 3 6.250 3.160 523 1.780.708 276.255.455 134.34.3.34 ICMP PING/ICMP 3 6.250 3.160 523 1.780.708 276.255.455 134.34.53.19 ICMP PING/ICMP 2 848 2.442 10 326.050 120.961.766 134.34.53.19 ICMP PING/ICMP 3 141.552 2.022 6 40.745 3.307.236 134.34.53.19 ICMP PING/ICMP 2 1.500 30 2.963 357.943 134.34.53.19 ICMP PING/ICMP 2 1.500 30 2.963 357.943 134.34.53.19 ICMP PING/ICMP 2 1.500 30 2.963 357.943	End Time 2008-04-03 00:0	134.34.53.42	ICMP Echo Reply,	4	172.917	8.197	8	88.135	62.855.538
Payload 1.238,35 GB 31.576 3.086,333 Source IP 2.877.353 134.34.53.135 (http_inspect) BA 3 1.255 3.648 9 31.576 3.086,333 Destination IP 2.890,423 134.34.53.135 (http_inspect) BA 3 1.255 3.649 9 31.576 5.00,845.863 Destination IP 2.890,423 134.34.53.135 (http_inspect) BA 3 6.250 3.160 523 1.780.076 278.255.455 Dottokup 3 6.250 3.160 523 1.780.076 278.255.455 134.34.53.152 CMP PING,ICMP 2 848 2.022 6 40.745 3.300.219 30.619.596 134.34.53.150 CMP PING,ICMP 3 9 1.191 7.999.080 217.171.129.125 ICMP PING,ICMP 3 9 1.991 13.436.315 217.999.080 217.171.129.125 1.0MP PING,ICMP 4 1.067 1.913 3.436.315 217.171.129.125 1.0MP PING,ICMP 4 1.067 1.913 3.436.315 217.171.129.125 1.0MP PING,ICMP 4 1.06	Packets 2.007.256.358	134.34.3.26	ICMP PING, ICMP	3	2.247	3.922	534	2.681.391	567.543.102
Source IP 2.877.353 134.34.34 COMP PING,ICMP 3 1.335 3.607 523 1.780.706 278.255.455 Destination IP 2.890.423 COMP PING,ICMP 3 6.220 3.160 523 1.780.706 278.255.455 Quick Lookup I34.34.34 ICMP PING,ICMP 2 848 2.425 10 326.050 129.961.766 I34.34.53.119 ICMP PENING Cyber 1 1 2.626 2.102 73.389 4.404.492 I34.345.51.166 ICMP PENING ICMP 3 141.552 2.002 6 40.745 3.307.236 I34.345.31.15 ICMP DEstination 1 44 1.886 490 2.86.003 17.999.080 I34.345.31.15 ICMP PENING ICMP 3 9 1.331 11 79.90.27.496.308 I34.345.31.15 ICMP PENING ICMP 3 9 1.331 11 79.90.27.496.308 I34.345.31.15 ICMP PING,ICMP 3 36 1.331 11 79.90.27.496.308 I34.345.33.165 ICMP PING,ICMP 3 37	Payload 1.238,35 GiB	134.34.53.135	(http_inspect) BA	3	21.566	3.648	9	31.571	3.086.333
Destination IP 2.890,423 134,34.3.34 ICMP PINS_(ICMP, 3 6,250 3.160 523 1.780,706 278,255,455 Quick Lookup 134,34.57,166 ICMP ENS_(ICMP, 6 1 2,625 2102 23 330,219 30,619,596 graddr -> dstaddr 134,34.53,119 ICMP ENS_(ICMP, 6 449 2.082 23 330,219 30,219 30,219 30,219 30,229 6 49,745 33,307,226 134,34,51,189,60 120,961,786 134,34,51,189,20 141,552 2.002 6 49,745 33,307,228 134,34,51,189,20 124,961,798,000 134,34,51,189,20 124,963,003 17,959,000 127,171,129,125 ICMP PINS_(ICMP, 2 2 1,500 30 2.963 557,943 134,34,53,160 ICMP PINS_(ICMP, 4 1,067 1,159 7 9,133 6,812,829 134,34,53,115 ICMP PINS_(ICMP, 4 1,067 1,159 7 9,133 6,812,829 134,34,53,115 ICMP PINS_(ICMP, 4 1,067 1,159 7 9,133 6,812,829 134,34,53,115 ICMP PINS_(ICMP, 4 1,067 1,159 7 9,133	Source IP 2.877.353	134.34.3.24	ICMP PING, ICMP	3	1.355	3.607	531	2.575.695	380.845.863
207.175.63.182 ICMP PING Cyber 1 1 2.625 2.102 73.389 14.04.492 134.34.53.166 ICMP Edio Reply 2 848 2.425 10 326.050 120.961.786 grcaddr -> dstaddr - 6 49 2.002 6 40.745 3.307.236 207.175.63.182 OK ISM PPING, ICMP P 3 141.552 2.022 6 40.745 3.307.236 134.34.53.19 ICMP PING, ICMP P 3 141.552 2.022 6 40.745 3.307.236 134.34.53.19 ICMP PING, ICMP P 3 141.552 2.022 6 40.745 3.307.236 134.34.53.15 ICMP PING, ICMP P 2 2 1.508 30 2.963 357.945 134.34.53.15 ICMP PING, ICMP P 4 1.067 1.199 7 9.183 6.812.6479 134.34.53.16 ICMP PING, ICMP P 6 8.224 843 7 2.495.308 134.34.53.161 ICMP PING, ICMP P 6 8.224 9 12.162 2.761.997	Destination IP 2.890.423	134.34.3.34	ICMP PING, ICMP	3	6.250	3.160	523	1.780.706	278.255.455
Quick Lookup 134.34.57.166 ICMP Etho Reply, 2 848 2.425 10 320.029 120.961.786 I34.34.57.166 ICMP Destination 6 49 2.082 23 330.029 120.961.786 I34.34.53.1182 I34.34.53.115 ICMP Destination 1 44 1.866 490 226.003 17.959.080 207.175.63.182 OK I34.34.53.15 ICMP PING,ICMP 2 2 1.508 30 2.963 557.943 134.34.53.150 ICMP PING,ICMP 3 9 1.391 11 78.902 72.4963 557.943 134.34.53.160 ICMP PING,ICMP 3 9 1.391 11 78.902 72.4963 166.479 134.34.53.160 ICMP PING,ICMP 6 8.224 843 7 2.435 166.479 134.34.53.161 ICMP PING,ICMP 6 8.224 843 7 2.435 166.479 134.34.53.165 ICMP PING,ICMP 6 8.224 843 7 2.435 166.479 134.34.53.165 ICMP PING,IC		207.175.63.182	ICMP PING Cyber	1	1	2.626	2.102	73.389	4.404.492
Quick Lookup 134.34.53.119 CMP Destination 6 49 2.082 26 30.219 30.619.596 srcaddr -> dstaddr still 189.69 CMP PING,ICMP 3 141.552 2.022 6 40.745 3.307.236 207.175.63.182 CMP PING,ICMP 1 1 44 1.865 490 226.003 17.959.080 134.34.53.15 ICMP PING,ICMP 2 2 1.508 30 2.963 557.943 134.34.53.160 ICMP PING,ICMP 3 9 1.391 11 78.902 72.496.308 134.34.53.151 ICMP PING,ICMP 4 1.067 1.159 7 9.133 6.81.282 134.34.53.160 ICMP PING,ICMP 6 8.224 843 7 2.485 166.479 134.34.53.151 ICMP ECho Reply 1 33 761 3 2.220 122.983 134.34.53.133 ICMP Liketineer 2 813 654 9 1.162 2.761.597 134.34.53.23 ICMP Liketineer 5 819 565 4 </td <th></th> <td>134.34.57.166</td> <td>ICMP Echo Reply,</td> <td>2</td> <td>848</td> <td>2.425</td> <td>10</td> <td>326.050</td> <td>120.961.786</td>		134.34.57.166	ICMP Echo Reply,	2	848	2.425	10	326.050	120.961.786
srcaddr -> dstaddr \$ 3 141.552 2.022 6 40.745 3.307.236 207.175.63.182 134.34.3.15 ICMP PINS,ICMP 1 4 1.856 490 226.003 17.959.080 207.175.63.182 OK 134.34.53.199 ICMP PINS,ICMP 2 2 1.908 30 2.963 157.943 134.34.53.199 ICMP PINS,ICMP 2 2 1.908 30 2.9208 30 2.9208 30 2.9208 30 2.9208 1.919 1.919 7 9 1.919 7 9 1.919 7 9 1.913 3.307 1.919 7 9 1.913 3 7 1.913 3 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913 1.913	Quick Lookup	134.34.53.119	ICMP Destination	6	49	2.082	23	330.219	30.619.596
134,34.3.15 ICMP Destination 1 44 1.656 490 226,003 17,959,080 207.175.63.182 IAMP PING,ICMP 2 2 1.508 30 2.963 57,943 Image: Construction of the prince of the p	srcaddr -> dstaddr	85.131.189.69	ICMP PING, ICMP	3	141.552	2.022	6	40.745	3.307.236
207.175.63.182 217.171.129.125 ICMP PING,ICMP 2 2 1.508 30 2.963 557,943 134.34.53.199 ICMP PING,ICMP 3 9 1.391 11 78.902 72.496.308 134.34.53.160 ICMP PING,ICMP 4 1.067 1.159 7 9.1391 7 7.485 7.66.403 7.785 7.786 7.766.403 7.741.133 134.34.53.133 ICMP L3retriever 5 819 555 4 722 7.4133 134.34.53.141 ICMP Etho Reply 6 27.735 495 8 3.150		134.34.3.15	ICMP Destination	1	44	1.856	490	236.003	17.959.080
Image: Constraint of the second se	207.175.63.182	217.171.129.125	ICMP PING, ICMP	2	2	1.508	30	2.963	557.943
OK 134.34.53.160 ICMP PING,ICMP 4 1.067 1.159 7 9.183 6.812.829 dstaddr Raw Records 134.34.53.115 ICMP PING,ICMP 6 8.224 843 7 2.485 166.479 134.34.53.115 ICMP PING,ICMP 6 8.224 843 7 2.485 166.479 134.34.53.115 ICMP PING,ICMP 6 8.224 843 7 2.485 166.479 134.34.53.133 ICMP L3retriever 2 813 654 9 12.162 2.761.597 134.34.53.133 ICMP L3retriever 2 813 654 9 12.162 2.761.597 134.34.53.133 ICMP L3retriever 5 819 565 4 782 74.133 134.34.53.50 ICMP L3retriever 3 19 483 6 12.379 2.980 134.34.53.50 ICMP L3retriever 3 19 483 6 12.379 2.980 134.34.53.81 SIMP public acces 2 10 391 7 18.752		134.34.53.199	ICMP PING, ICMP	3	9	1.391	11	78.902	72.496.308
dstaddr Raw Records 207.175.63.182 OK 134.34.53.115 ICMP PING,ICMP 6 8.224 843 7 2.485 166.479 134.34.53.165 ICMP Echo Reply 1 33 761 3 2.220 122.983 134.34.53.182 OK 134.34.53.23 ICMP L3retriever 2 813 654 9 7.786 756.403 134.34.53.23 ICMP L3retriever 2 813 654 9 12.162 2.761.597 134.34.53.23 ICMP L3retriever 5 819 555 4 782 74.133 134.34.53.50 ICMP L3retriever 5 819 555 8 3.150 344.316 134.34.53.182 OK IMP L3retriever 3 19 483 6 12.379 2.980.333 134.34.53.141 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SIMP public acces 2 10 391 7 18.267 1.841.193 134.34.53.141	OK	134.34.53.160	ICMP PING, ICMP	4	1.067	1.159	7	9.183	6.812.829
dstaddr I Raw Records 207.175.63.182 OK Network Tools 134.34.53.165 ICMP Echo Reply 1 33 761 3 2.220 122.983 WHOIS I34.34.53.133 ICMP Laretriever 2 813 654 9 12.162 2.761.597 134.34.53.133 ICMP Laretriever 5 819 565 4 762 74.133 134.34.53.133 ICMP Echo Reply 6 27.735 495 8 3.150 344.316 134.34.53.58 ICMP Laretriever 3 19 483 6 12.379 2.980.333 134.34.53.50 ICMP Laretriever 3 21 439 8 3.743 1.875.266 134.34.53.141 ICMP Laretriever 3 21 439 8 3.743 1.875.266 134.34.53.141 ICMP Laretriever 3 21 439 8 3.743 1.875.266 134.34.53.141 ICMP PING ICMP 2 11 388 353 978 38.436 65.114.168.150 I		134.34.53.115	ICMP PING, ICMP	6	8.224	843	7	2.485	166.479
207.175.63.182 OK 3 23 669 6 7.786 796.403 134.34.53.83 SHELCODE x86 2 813 654 9 12.162 2.761.597 134.34.53.133 ICMP L3retriever 5 819 565 4 782 74.133 134.34.53.133 ICMP L3retriever 5 819 565 4 782 74.133 134.34.53.133 ICMP L3retriever 6 27.735 495 8 3.150 344.316 134.34.53.58 ICMP L3retriever 3 19 483 6 12.379 2.980.333 134.34.53.58 ICMP L3retriever 3 21 439 8 3.743 1.875.66 207.175.63.182 OK ICMP L3retriever 3 21 439 8 3.743 1.875.66 207.175.63.182 OK ICMP PING,ICMP 2 10 391 7 18.267 1.841.193 134.34.53.141 ICMP PING,ICMP 2 11 388 353 978 3.8.436 65.11	dstaddr 💌 🛛 Raw Records	134.34.53.165	ICMP Echo Reply	1	33	761	3	2.220	122.983
134.34.53.102 134.34.53.223 ICMP L3retriever 2 813 654 9 12.162 2.761.597 INetwork Tools 134.34.53.133 ICMP L3retriever 5 819 565 4 782 74.133 IWHOIS I34.34.53.58 ICMP L3retriever 6 27.735 495 8 3.150 344.316 134.34.53.58 ICMP L3retriever 3 19 483 6 12.379 2.980.333 134.34.53.50 ICMP L3retriever 2 3 481 8 1.620 169.102 207.175.63.182 OK I34.34.53.141 ICMP L3retriever 2 3 481 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING, ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING, ICMP 2 15	207 175 63 182 OK	134.34.53.83	SHELLCODE x86	3	23	659	6	7.786	756.403
Network Tools 134.34.53.133 ICMP L3retriever 5 819 565 4 782 74.133 WHOIS 134.34.53.477 ICMP Echo Reply, 6 27.735 495 8 3.150 344.316 134.34.53.58 ICMP L3retriever 3 19 483 6 12.379 2.980.333 134.34.53.50 ICMP L3retriever 2 3 481 8 1.620 169.102 207.175.63.182 OK 134.34.53.141 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING, ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING, ICMP 2 15 372 355 373		134.34.53.223	ICMP L3retriever	2	813	654	9	12.162	2.761.597
Network Tools 134.34.53.47 ICMP Echo Reply, 6 27.735 495 8 3.150 344.316 WHOIS I34.34.53.58 ICMP L3retriever 3 19 483 6 12.379 2.980.333 207.175.63.182 OK I34.34.53.50 ICMP L3retriever 2 3 481 8 1.620 169.102 134.34.53.141 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING,ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628 Image: Comparison of the comparison		134.34.53.133	ICMP L3retriever	5	819	565	4	782	74.133
WHOIS I34.34.53.58 ICMP L3retriever 3 19 483 6 12.379 2.980.333 207.175.63.182 OK I34.34.53.50 ICMP L3retriever 2 3 481 8 1.620 169.102 207.175.63.182 OK I34.34.53.141 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING, ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING, ICMP 2 15 372 355 373 15.628	Network Tools	134.34.53.47	ICMP Echo Reply,	6	27.735	495	8	3.150	344.316
WHOIS 134.34.53.50 ICMP L3retriever 2 3 481 8 1.620 169.102 207.175.63.182 OK 134.34.53.50 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING, ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING, ICMP 2 15 372 355 373 15.628 Image: Comparison of the compariso		134.34.53.58	ICMP L3retriever	3	19	483	6	12.379	2.980.333
207.175.63.182 OK 134.34.53.141 ICMP L3retriever 3 21 439 8 3.743 1.875.266 134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING, ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING, ICMP 2 15 372 355 373 15.628 V	WHOIS	134.34.53.50	ICMP L3retriever	2	3	481	8	1.620	169.102
134.34.53.81 SNMP public acces 2 10 391 7 18.267 1.841.193 65.114.168.150 ICMP PING,ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628 Image: Comparison of the compariso	207.175.63.182 OK	134.34.53.141	ICMP L3retriever	3	21	439	8	3.743	1.875.266
65.114.168.150 ICMP PING,ICMP 2 11 388 353 978 38.436 65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628		134.34.53.81	SNMP public acces	2	10	391	7	18.267	1.841.193
65.114.168.151 ICMP PING 1 5 379 361 384 16.458 65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628		65.114.168.150	ICMP PING, ICMP	2	11	388	353	978	38.436
65.114.168.149 ICMP PING NMAP 1 7 377 362 381 16.194 65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628		65.114.168.151	ICMP PING	1	5	379	361	384	16.458
65.114.168.148 ICMP PING,ICMP 2 15 372 355 373 15.628		65.114.168.149	ICMP PING NMAP	1	7	377	362	381	16.194
		65.114.168.148	ICMP PING, ICMP	2	15	372	355	373	15.628 🖵
Visual Connection Analysis I Ignore single flow connections V Include any traffic between hosts		Visual Connect	ion Analysis	Ianore single flow conr	ections 🔽 Include	any traffic between h	nosts		

Intrusion Detection View – Suspicious Hosts



File Tools Export Data Help



Home-Centric Network Visualization

🕌 NFlowVis

File Tools Export Data Help



Graph Visualization

🚣 NFlowVis

File Tools Export Data Help



Host Details View

🛃 NFlowVis

File Tools Export Data Help

NFlowVis

NetFlow Visualization Tool

1. Overview 2. Intrusion Detection View 3a. Flow Visualization 3b. Graph 4. Host Details 5. NetFlow Records

NetFlow Raw Records

	timestamp	dpkts	doctets srcaddr	dstaddr	srcport	dstport	prot 🛆
	2008-04-02 00:22:25	9	1.015 85.131.189.69	134.34.53.119	36805	443	6 🔺
Durational Colombian	2008-04-02 00:22:27	5	256 85.131.189.69	134.34.53.119	33377	1194	6
Project Selection	2008-04-02 00:22:27	7	384 85, 131, 189, 69	134.34.53.119	60193	22	6
2008-04-02	2008-04-02 00:27:27	7	398 85.131.189.69	134.34.53.119	43093	25	6
	2008-04-02 00:27:27	8	963 85.131.189.69	134.34.53.119	37439	443	6
Attribute Value	2008-04-02 00:27:27	4	210 85.131.189.69	134.34.53.119	33758	1194	6
Flows 108.142.800	2008-04-02 00:27:30	6	338 85, 131, 189, 69	134.34.53.119	34426	22	6
Start Time 2008-04-01 23:5	2008-04-02 00:27:30	9	903 85.131.189.69	134.34.53.119	37972	993	6
End Time 2008-04-03 00:0	2008-04-02 00:27:29	6	338 85, 131, 189, 69	134.34.53.119	34426	22	6
Packets 2.007.256.358	2008-04-02 00:27:29	8	963 85.131.189.69	134.34.53.119	37439	443	6
Payload 1.238,35 GiB	2008-04-02 00:27:29	4	210 85.131.189.69	134.34.53.119	33758	1194	6
Source IP 2.877.353	2008-04-02 00:27:31	7	398 85.131.189.69	134.34.53.119	43093	25	6
Destination IP 2.890.423	2008-04-02 00:27:31	9	903 85.131.189.69	134.34.53.119	37972	993	6
,	2008-04-02 00:32:23	7	398 85.131.189.69	134.34.53.119	54749	25	6
- · · · ·	2008-04-02 00:32:23	9	1.015 85.131.189.69	134.34.53.119	55930	443	6
Quick Lookup	2008-04-02 00:32:23	6	338 85, 131, 189, 69	134.34.53.119	46144	22	6
srcaddr -> dstaddr 🔹	2008-04-02 00:32:27	4	210 85.131.189.69	134.34.53.119	37860	1194	6
	2008-04-02 00:32:27	7	398 85, 131, 189, 69	134.34.53.119	54749	25	6
85.131.189.69	2008-04-02 00:32:27	6	338 85, 131, 189, 69	134.34.53.119	46144	22	6
134 34 53 119 OK	2008-04-02 00:32:27	10	955 85.131.189.69	134.34.53.119	48410	993	6
134.34.33.115	2008-04-02 00:32:27	9	1.015 85.131.189.69	134.34.53.119	55930	443	6
dstaddr 👻 Raw Records	2008-04-02 00:32:26	10	955 85, 131, 189, 69	134.34.53.119	48410	993	6
	2008-04-02 00:32:26	4	210 85.131.189.69	134.34.53.119	37860	1194	6
85.131.189.69 OK	2008-04-02 00:37:23	4	210 85.131.189.69	134.34.53.119	43301	1194	6
	2008-04-02 00:37:27	7	384 85, 131, 189, 69	134.34.53.119	54692	22	6
	2008-04-02 00:37:27	8	963 85.131.189.69	134.34.53.119	44807	443	6
Network Tools	2008-04-02 00:37:27	7	398 85.131.189.69	134.34.53.119	48062	25	6
WHOIS	2008-04-02 00:37:27	10	955 85.131.189.69	134.34.53.119	38808	993	6
	2008-04-02 00:37:27	4	210 85, 131, 189, 69	134.34.53.119	43301	1194	6
207.175.63.182 OK	2008-04-02 00:37:31	7	398 85.131.189.69	134.34.53.119	48062	25	6
	2008-04-02 00:37:31	7	384 85.131.189.69	134.34.53.119	54692	22	6
	2008-04-02 00:37:31	8	963 85.131.189.69	134.34.53.119	44807	443	6
	2008-04-02 00:37:31	10	955 85.131.189.69	134.34.53.119	38808	993	6
	2008-04-02 00:42:24	6	338 85, 131, 189, 69	134.34.53.119	44091	22	6
	2008-04-02 00:42:24	7	398 85, 131, 189, 69	134.34.53.119	33967	25	6
	2008-04-02 00:42:24	10	955 85.131.189.69	134.34.53.119	34455	993	6
	2008-04-02 00:42:24	4	210 85, 131, 189, 69	134.34.53.119	53414	1194	6 🔻
	,						LIMIT 100

NetFlow Records

Service Monitoring with NFlowVis

- Example: Conficker Worm (11/2008)
- Exploits MS08-067 vulnerability
- RPC over Port 445/TCP

 Are there any compromised hosts in my network?



🛓 NFlowVis

File Tools Export Data Help

ow Visualization Tool	DS Data Source			
	Conficker Related Behavior (MS08-067)			
	Suspicious Hosts Template Settings			
ct Selection				
9-01-29	Refresh Host List			
	srcaddr	Distinct Destination Hosts	Packets	Octoto
Attribute Value	134 34 16 106	9 433	506 528	24 737 22
s 160.169.017	134 34 16 100	2 740	506.520	24,737,23
t Time 2009-01-29 00:0	124 24 16 4	2.629	401.020	27,031,30
Time 2009-01-30 00:0	124 24 16 105	1 072	169 502	23,003,00
ets 4.736.715.468	134 34 16 111	1.075	175 601	9 720 27
oad 3.406,91 GiB	124 24 16 126	650	2.005	179.77
ce IP 4.352.179	124 24 9 122	24	2,555	277.090.02
ination IP 4.438.678	124 24 110 251		200.091	7 02
	134 34 120 14	0	7 440	1 270 15
	124 24 120 15		12 609	7 202 62
Lookup	124 24 120 15		20.651	2.490.02
ldr -> dstaddr 🔹	124 24 120 5	5	20.001	2.105.03
	124 24 120 7		10.750	1 722 47
	124 24 120 9		27.412	4 500 57
	134 34 120.0	5	156 222	82 260 12
	124 24 120 10		07.620	107 110 29
ddr 🔻 🗖 Raw Records	134 34 120 11		142 275	175 240 51
	134 34 120 12	5	61 076	0 745 00
ОК	124 24 120 12		26.022	2,75,00
	134 34 120 37	5	20.955	20.034.03
	124 24 120.0		1 507 114	2.007.00
ork Tools	124 24 120 1		1,377,117 527,520	2,090,901,13
IS 👻	124 24 110 205		27	2.04
	124 24 120 2		6 525	1 120 76
ОК	134.34,120.2		6.000	1,130,70
	124 24 120 4	5	0,992	264 206 62
	134.34.120.0		204.104 6.607	207.300.02
	124 24 120 19	5	6.03	1,136,73
	124 24 120 10	5	0.003	1.048.31
	154.54.120.19	5	27.158	5,949,68
	Visual Connection Analysis	🔽 Iapore single flow connections . 🗖 Include any tr	affic between bosts	

Intrusion Detection View – Suspicious Hosts



File Tools Export Data Help



Home-Centric Network Visualization

Analyzing SSH Attacks with NFlowVis



http://stats.denyhosts.net/stats.html

 How was our network affected by these attacks?



NFlowVis

Flows

File Tools Export Data Help

1.090.036

1. Overview 2. Intrusion Detection View 3a, Flow Visualization 3b, Graph 4. Host Details 5. NetFlow Records NFlowVis **NetFlow Visualization Tool** IDS Data Source Brute Scan Attacker (SSH) Suspicious Hosts | Template Settings | Project Selection Refresh Host List Ŧ 2009-10-05 srcaddr Packets Octets Distinct Destination Hosts Attribute Value 120.195.80.119 2.441 17.106 1.452.430 203.278.742 125.71.206.167 2.337 153.614 3.201 Start Time 2009-10-05 00:0... 119.73.139.231 1.566 4.206 300.474 End Time 2009-10-06 00:0... 189,62,40,78 956 1.291 61.942 Packets 4.105.251.152 403.436 122.160.7.94 903 6.751 2.477,22 GiB Payload 190.36.176.250 838 1.133 54.372 3.853.700 Source IP 200.49.223.68 5.620 489.906 752 3.773.942 Destination IP 220.227.25.211 715 974 46.740 218.87.32.241 572 617 29.616 24.40.132.121 175 247 11.856 Quick Lookup 134.208.3.105 152 228 10.944 srcaddr -> dstaddr Ŧ 41.204.56.146 114 557 33.406 103 7.993 58.185.182.203 751.376 12.152.56.195 58.233.219.96 103 2.236 203.042 183,188 59.37.75.238 103 1.992 OK 59.37.75.241 103 13.247 1.242.082 Raw Records dstaddr \mathbf{w} 59.40.185.96 103 9.087 853.172 59.162.166.50 103 12.273 1.155.090 12.152.56.195 OK 59.162.166.51 103 10.420 975.016 60.31.197.99 103 249.150 2.988 60.240.249.116 103 10.027 933.204 Network Tools 61.107.16.33 103 18.230 1.707.096 WHOIS Ŧ 61.158.154.8 996.634 103 10.541 61.166.150.117 103 9,464 888.770 120.195.80.119 OK 61.172.200.70 103 6.916 649.584 61.235.143.231 103 6.161 573.114 62.151.177.10 103 17.852 1.685.986 62.221.52.251 175.702 103 1.873

Visual Connection Analysis

62.245.152.234

103

11.534

Remote Hosts with SSH connections (5th October 2009)

🕌 NFlowVis

File Tools Export Data Help



- 🗆 ×

Home-Centric Network Visualization



File Tools Export Data Help

2009-10-05

Flows

Start Time

End Time

Packets

Payload

Source IP

Destination IP

Quick Lookup

12.152.56.195

12.152.56.195

Network Tools

120.195.80.119

WHOIS

 \mathbf{w}

dstaddr

Attribute



Home-Centric Network Visualization (Drill-Down)

Ŧ

134.34.13.0/24

134.34.25.0/24 134.34.33.0/24

÷ +…

+...



File Tools Export Data Help



Home-Centric Network Visualization (Drill-Down)

🕌 NFlowVis

File Tools Export Data Help



Graph Visualization



Home-Centric Network Visualization (SSH Attacks on 5th October 2009)



Graph Visualization (SSH Attacks on 5th October 2009)

Conclusions

- Intrusion Detection and Network Monitoring combined
- Automated Analysis combined with Interactive Exploration

 NFlowVis is a Visual Analytics System for Network Data



Thank you very much for your attention!

Questions?

For further information about this work please contact

Fabian Fischer Tel. +49 7531 88-2780 Fabian.Fischer@uni-konstanz.de

http://nflowvis.dbvis.de/



References I



Ball, R., Fink, G., and North, C. (2004).

Home-centric visualization of network traffic for security administration.

Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, pages 55–64.



Holten, D. (2006).

Hierarchical Edge Bundles: Visualization of Adjacency Relations in Hierarchical Data.

IEEE Trans. Vis. Comput. Graph., 12(5):741–748.



References II



Ellson, J., Gansner, E., Koutsofios, L., North, S., and Woodhull, G. (2002).

Graphviz-Open Source Graph Drawing Tools.

Lecture Notes in Computer Science, pages 483–484.



Shneiderman, B. (1992).

Tree visualization with tree-maps: 2-d space-filling approach. *ACM Trans. Graph.*, *11*(1):92–99.



Hierarchical Edge Bundling





Hierarchical Edge Bundling



