

Using Geographic Information Systems for Enhanced Security Visualization

> Matthew Dunlop David Shelly

Agenda

- Purpose
- Problem
- Study
 - Design
 - Results
- Prototype
- Future

Purpose

- To design a usable security visualization prototype tool that leverages global information systems (GIS)
 - Present security information more clearly
 - Facilitate rapid identification of network security shortcomings
 - Allow better protection of critical network assets

Problem

- Information overload
 - VT processes over 5 million emails per day
 - Manages over 500 SMTP & 3500 HTTP servers
- Analysts rely on multiple tools
 - Analysis takes more time
- Popular tools are not very usable
 - Primarily text based
 - Do not scale well for large networks
 - Graphical representations are not intuitive
- GIS adds context as well as scalability

Current Security Tools – Text-based

Snort

M e n u		Snortkep	at						
Tim Curr Unic Num	efram rent T que Si nber o	e: 2003-07-16 20:05:08 to 2003-07-19 20:05:12 ime: 2003-07-19 20:05:12 gradures: 11 f Alerts: 131	Types of Traffic 61.8% □ TCP (81) □ UDP (0) □						
Earliest Alert: 2003-07-16 20:21:17 Latest Alert: 2003-07-19 12:07.26									
Day: CO 0.02 38.22									
Detail by Signatures									
Nur	n Prio	Signature	# Alerts	# Sources	# Dest.	Detail			
1	1	WEB-CLIENT javascript URL host spoofing attempt [sid 1841] [bugtraq 5293]	2	1	1	Summary			
-									
2	2	SCAN SOCKS Proxy attempt [sid 615] [url help.undernet.org/proxyscan/]	59	12	5	Summary			
2 3	2 2	SCAN SOCKS Proxy attempt [sid 615] [url help.undernet.org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311]	59 32	12	5 1	Summary Summary			
2 3 4	2 2 2	SCAN SOCKS Proxy attempt [sid 615] [url help.undernet.org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618]	59 32 6	12 1 1	5 1 1	Summary Summary Summary			
2 3 4 5	2 2 2 2	SCAN SOCKS Proxy attempt [sid 615] [url help undernet org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618] DDOS mstream handler to client [sid 248] [cve CAN-2000-0138]	59 32 6 6	12 1 1 1	5 1 1 1	Summary Summary Summary Summary			
2 3 4 5 6	2 2 2 2 2 2	SCAN SOCKS Proxy attempt [sid 615] [url help undernet.org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618] DDOS mstream handler to client [sid 248] [cve CAN-2000-0138] SCAN Proxy (8080) attempt [sid 620]	59 32 6 6 6 6	12 1 1 1 1 1	5 1 1 1 1	Summary Summary Summary Summary Summary			
2 3 4 5 6 7	2 2 2 2 2 2 2	SCAN SOCKS Proxy attempt [sid 615] [url help undernet.org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618] DDOS mstream handler to client [sid 248] [cve CAN-2000-0138] SCAN Proxy (6080) attempt [sid 620] ICMP Large ICMP Packet [sid 499] [arachnids 246]	59 32 6 6 6 6 6	12 1 1 1 1 2	5 1 1 1 1 1	Summary Summary Summary Summary Summary Summary			
2 3 4 5 6 7 8	2 2 2 2 2 2 2 3	SCAN SOCKS Proxy attempt [sid 615] [url help undernet org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618] DDOS mstream handler to client [sid 248] [cve CAN-2000-0138] SCAN Proxy (8080) attempt [sid 620] ICMP Large ICMP Packet [sid 499] [arachnids 246] ICMP Destination Unreachable (Communication Administratively Prohibited) [sid 485]	59 32 6 6 6 6 6 10	12 1 1 1 2 4	5 1 1 1 1 1 1 1 1	Summary Summary Summary Summary Summary Summary Summary			
2 3 4 5 6 7 8 9	2 2 2 2 2 2 3 3 3	SCAN SOCKS Proxy attempt [sid 615] [url help undernet.org/proxyscan/] ICMP L3retriever Ping [sid 466] [arachnids 311] SCAN Squid Proxy attempt [sid 618] DDOS mstream handler to client [sid 248] [cve CAN-2000-0138] SCAN Proxy (8080) attempt [sid 620] ICMP Large ICMP Packet [sid 499] [arachnids 246] ICMP Destination Unreachable (Communication Administratively Prohibited) [sid 485] ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited) [sid 487]	59 32 6 6 6 6 6 10 2	12 1 1 1 1 2 4 2	5 1 1 1 1 1 1 1 1 1 1	Summary Summary Summary Summary Summary Summary Summary Summary			

Page finished: July 19, 2003, 20:05:08 Page finished: July 19, 2003, 20:05:12

> Snort Report Version 1.2 Copyright 2000-2003, <u>Circuits Maximus, LLC.</u>

Wireshark

🚺 (Untitled) - Wireshark										
<u>File Edit View G</u>	io <u>C</u> apture <u>A</u> nalyze <u>S</u> ta	atistics Telephony <u>T</u> ools <u>H</u> e	elp							
	K 🖻 🖬 🗙 😂 🗏] 🔍 🗢 🗢 🖗 🖉 💆		⊕ , ⊖ , »						
Filter:		Expression	Clea <u>r</u> App <u>ly</u>							
No Time	Source	Destination	Protocol	Info						
212 3.090200	200-00-00-000	100 - 100 -	SSUP	NUITER .						
213 3.911931	198.42.99.135	238.255.255.250	SSDP	NOTIFY *						
214 3.911994	198.82.99.115	238,255,255,250	SSDP	NOTIFY *						
215 3.946516	101 Teche, 87 (10-100	Broadcast.	ARP	Who has :						
216 4.022255	198.82.99.135	238.235.255.250	SSDP	NOTIFY *						
21/ 4.022346	1 MA. 84. 88. 1.17	1 10. 1 10. 1 10. 1 10.	SSDP	NOTIFY *						
218 4.023418	1 Mar. 40. 40. 111	2 Mar. 2 Mar. 2 Mar. 2 Mar.	SSDP	NOTIFY *						
219 4.023403	100.01.00.110	220 225 255 255	SSUP	NOTIFY *						
220 4.040815	100 01 00 110	200 200 200 200	SSOP	NOTIFY #						
222 4.040300	10011 011 100 000	Br candy and	APP	who has '						
223 4 085255	100.01.00.100	200 200 200 200	SSOP	NOTTEX *						
224 4 085340	100.01.00.111	238 255 255 250	SSDP	NOTTEY *						
225 4.086747	198 81 188 150	238,255,255,250	SSDP	NOTTEY *						
226 4.087722	198 82 188 190	238,255,255,250	SSDP	NOTIFY *						
227 4.115166	198, 42, 99, 125	239.255.255.259	SSDP	NOTIFY * -						
🗄 Frame 1 (368 bytes on wire, 368 bytes captured)										
B Ethernet II, Src: Cisco and a second secon										
Internet Pro	tocol, Src:	99.135 (198.82.99.135	5. max: 21	18.255.255.						
User Datagram Protocol Src Port: ssdp (1900) Dst Port: ssdp (1900)										
B by artest Transfer Protocol										
a hypercext II										
100-0										
				F.						
0000										
0010	47 00 00 01 11 44	75 28 52 63 67 47 77								
0020	AL OF AL OL AN AL	32 44 47 34 49 48 39		AL, 2MOTTO						
K										
C, File: "C:\Users" AppData\Local\Temp\ Packets: 230 Displayed: 23										

Current Security Tools – Graphical

The Network Visualizer

Rumint



Study Design - Participants

- Virginia Tech system administrators
- SANS IT professionals
- U.S. Army network engineers



50 respondents

Study Design – Question Areas

- Background Information
- System Information
- Security Information
- Security Tools
- GIS Information

Study Results – Background



Study Results - Preferences

Most important aspects of security tools



- Top usability improvements
 - Improved user interface
 - Better summary of information
 - Improved visual representation
- Other findings
 - Prefer customizability
 - Multiple tools = longer
 time to isolate threats

Study Results - Visualization

- Visualization not widely used
 - 50% never used it to visualize networks
 - 76% never used it to visualize security
- Openness to GIS visualization
 - 76% feel GIS tool would be useful for network visualization
 - □ 50% envision using it for security visualization
- Helpful in explaining security to technical and nontechnical audiences



Detailed View



Future Work

- Build working model of prototype
- Conduct usability study



