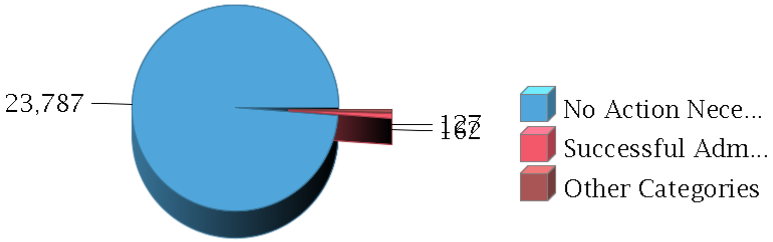
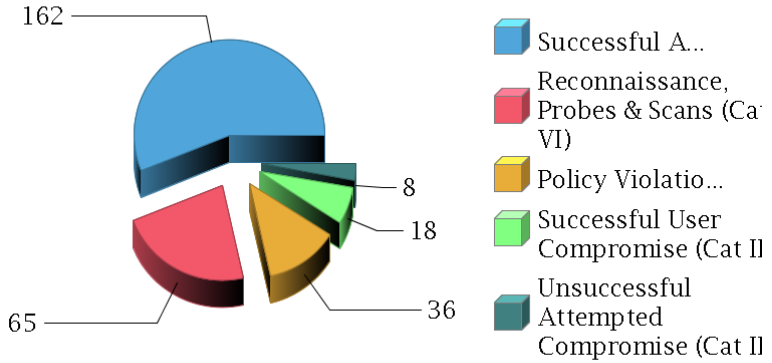
Alerts Categorized During Report Period

Alert Categorizations



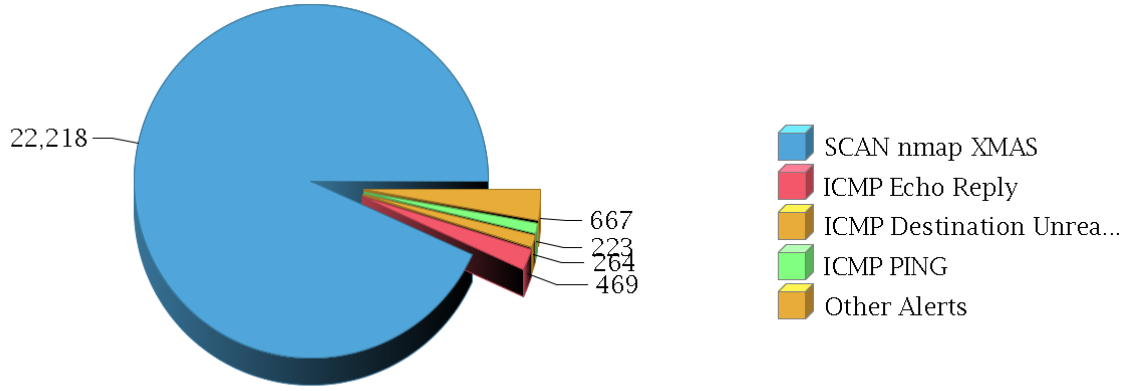
Malicious Activity Detail



Status	Count
No Action Necessary (Cat VIII)	23787
Successful Admin Compromise (Cat I)	162
Reconnaissance, Probes & Scans (Cat VI)	65
Policy Violation or Poor Security Practice (Cat V)	36
Successful User Compromise (Cat II)	18
Unsuccessful Attempted Compromise (Cat III)	8

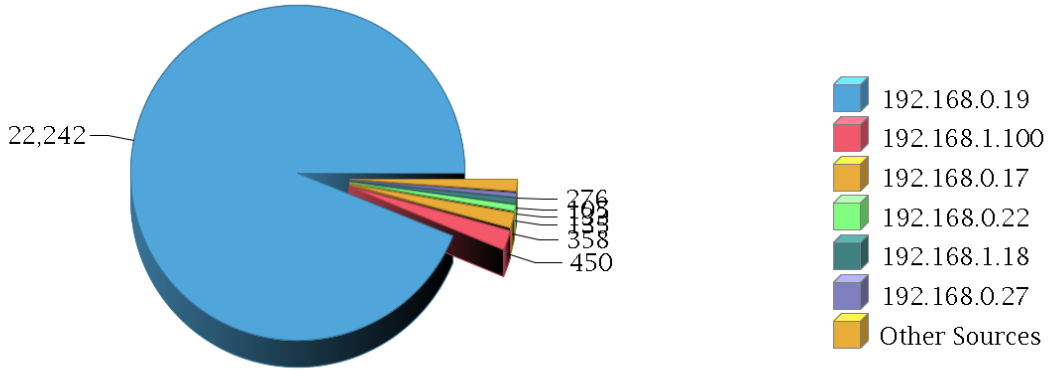
Report generated on Apr 17, 2007 2:30 PM

Most Frequent Alerts



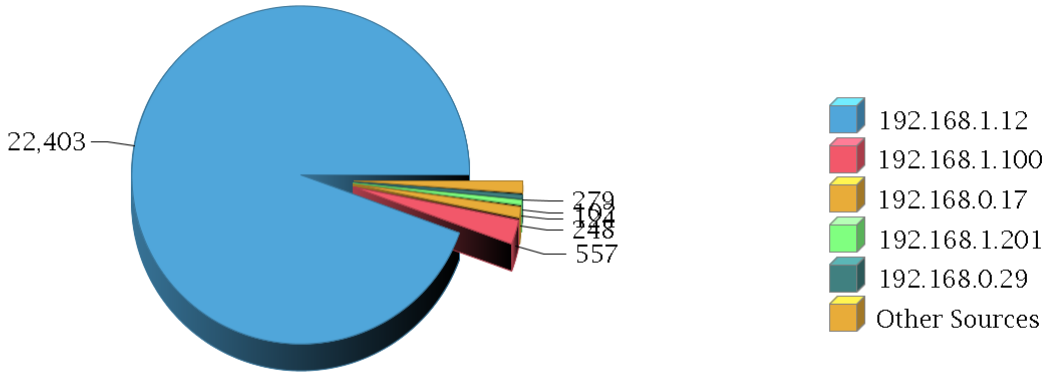
Alert	Count
SCAN nmap XMAS	22218
ICMP Echo Reply	469
ICMP Destination Unreachable Port Unreachable	264
ICMP PING	223
ICMP PING BSDtype	175
ICMP PING *NIX	175
portscan: Open Port	149
portscan: TCP Portscan	59
SNMP trap tcp	55
SNMP request tcp	54

Top Sources of Alerts



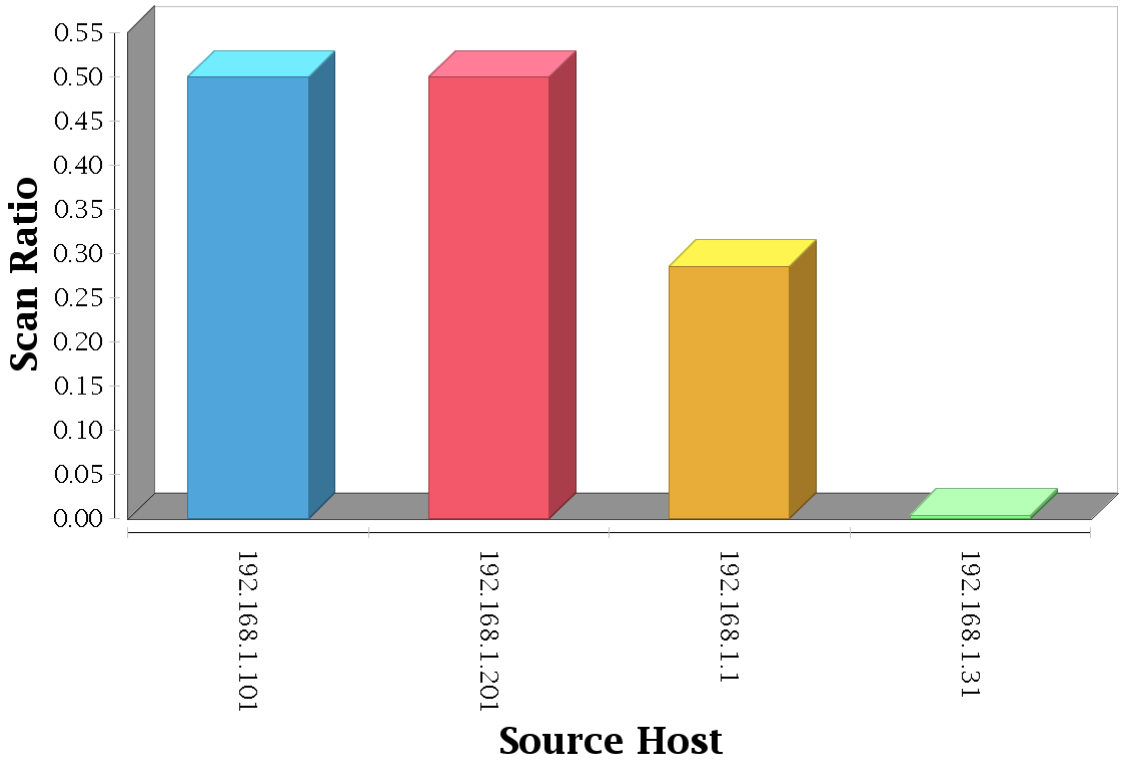
Source	Hostname	Count
192.168.0.19	192.168.0.19	22242
192.168.1.100	192.168.1.100	450
192.168.0.17	192.168.0.17	358
192.168.0.22	192.168.0.22	135
192.168.1.18	192.168.1.18	133
192.168.0.27	192.168.0.27	105
192.168.0.28	192.168.0.28	98
192.168.1.11	192.168.1.11	67
192.168.0.26	192.168.0.26	59
192.168.0.21	192.168.0.21	52

Top Destinations of Alerts



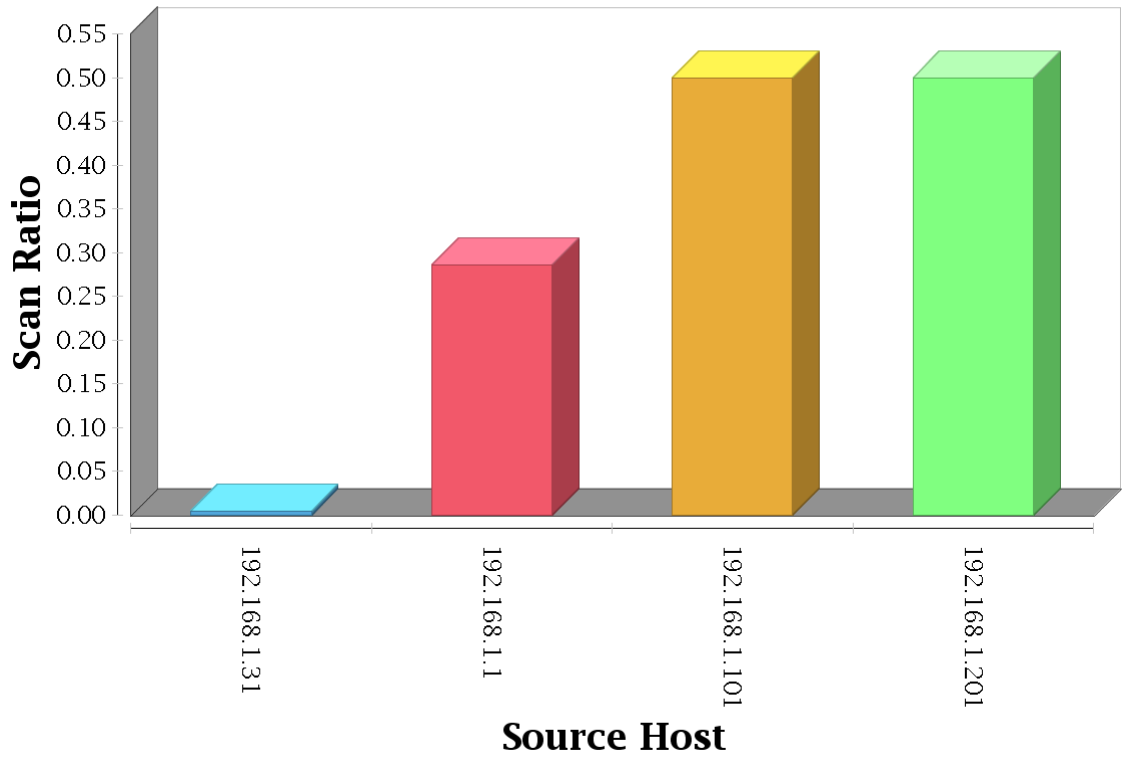
Destination	Hostname	Count
192.168.1.12	192.168.1.12	22403
192.168.1.100	192.168.1.100	557
192.168.0.17	192.168.0.17	248
192.168.1.201	192.168.1.201	124
192.168.0.29	192.168.0.29	102
192.168.1.200	192.168.1.200	68
192.168.186.1	192.168.186.1	63
192.168.59.1	192.168.59.1	60
192.168.0.26	192.168.0.26	45
192.168.1.13	192.168.1.13	43

Top Internal Portsweepers



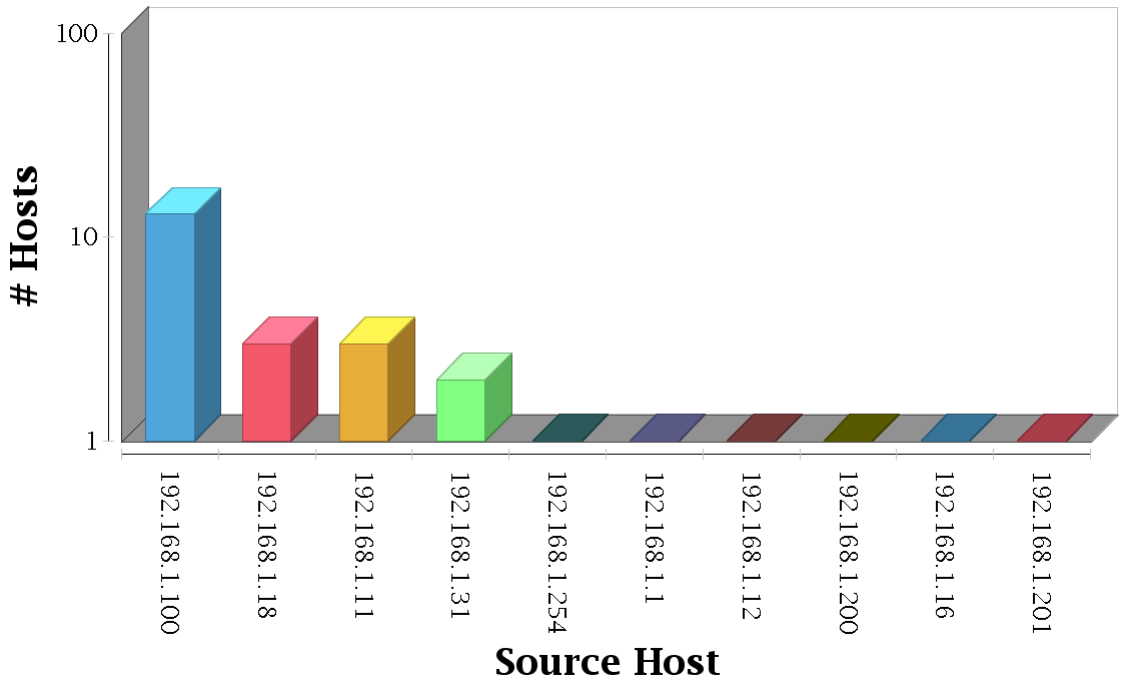
Source	Source Hostname	# Dests	# Ports	Scan Ratio
192.168.1.101	192.168.1.101	1	2	0.5
192.168.1.201	192.168.1.201	1	2	0.5
192.168.1.1	192.168.1.1	2	7	0.286
192.168.1.31	192.168.1.31	7	1698	0.004

Top Internal Portscanners



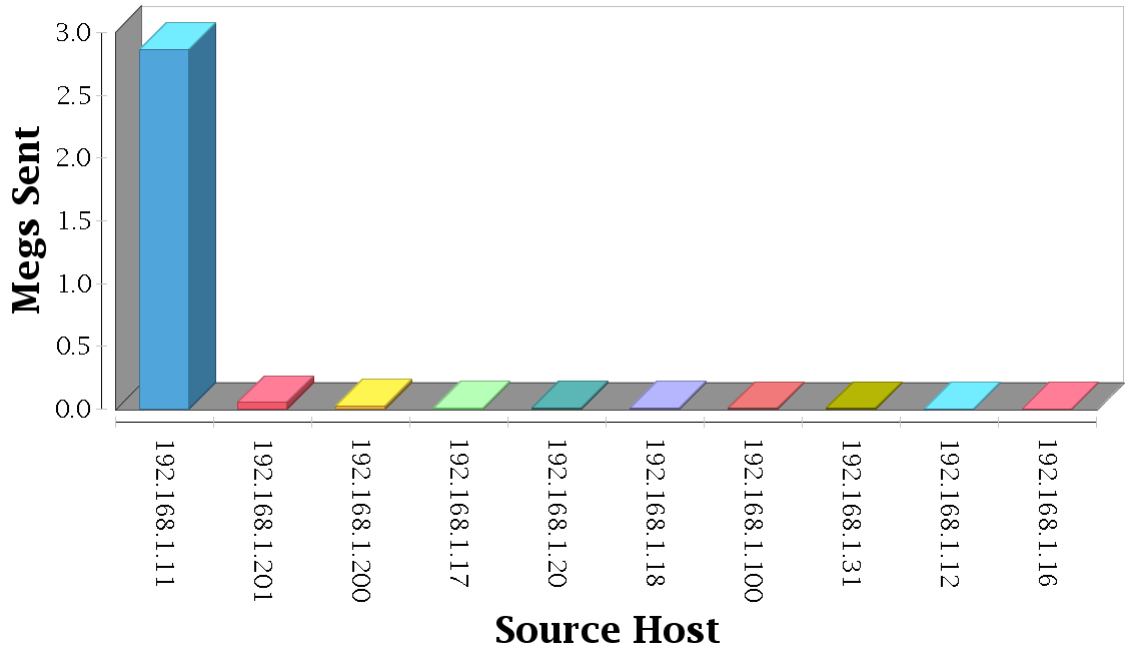
Source	Source Hostname	# Destinations	# Ports	Scan Ratio
192.168.1.31	192.168.1.31	7	1698	0.00
192.168.1.1	192.168.1.1	2	7	0.29
192.168.1.101	192.168.1.101	1	2	0.50
192.168.1.201	192.168.1.201	1	2	0.50

Top Internal Pingsweepers



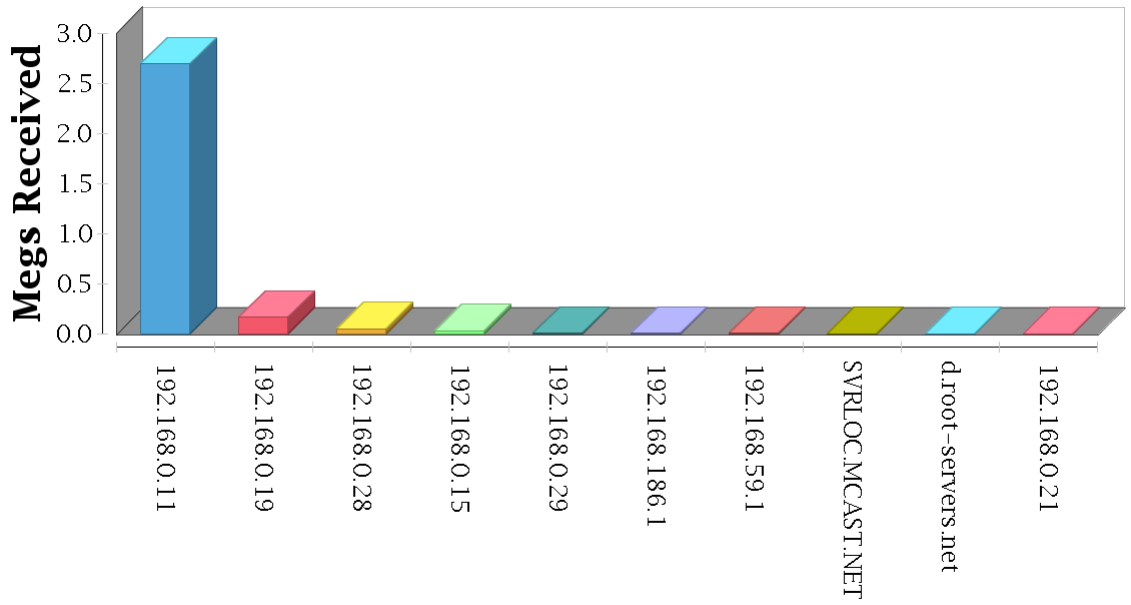
Source	Source Hostname	# Destinations
192.168.1.100	192.168.1.100	13
192.168.1.18	192.168.1.18	3
192.168.1.11	192.168.1.11	3
192.168.1.31	192.168.1.31	2
192.168.1.254	192.168.1.254	1
192.168.1.1	192.168.1.1	1
192.168.1.12	192.168.1.12	1
192.168.1.200	192.168.1.200	1
192.168.1.16	192.168.1.16	1
192.168.1.201	192.168.1.201	1

Top Systems Sending Data Offsite



Source	Source Hostname	# External Hosts	Megs Transferred
192.168.1.11	192.168.1.11	6	3
192.168.1.201	192.168.1.201	9	0
192.168.1.200	192.168.1.200	4	0
192.168.1.17	192.168.1.17	14	0
192.168.1.20	192.168.1.20	1	0
192.168.1.18	192.168.1.18	3	0
192.168.1.100	192.168.1.100	22	0
192.168.1.31	192.168.1.31	2	0
192.168.1.12	192.168.1.12	4	0
192.168.1.16	192.168.1.16	2	0

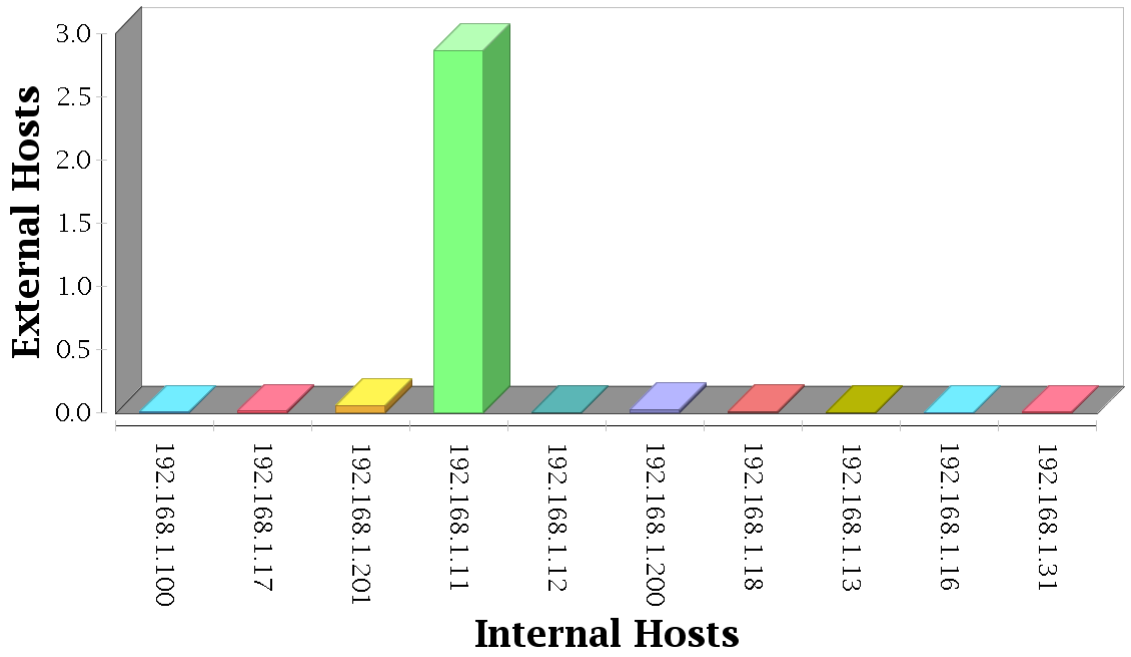
Top Offsite Systems Receiving Data



External Hosts

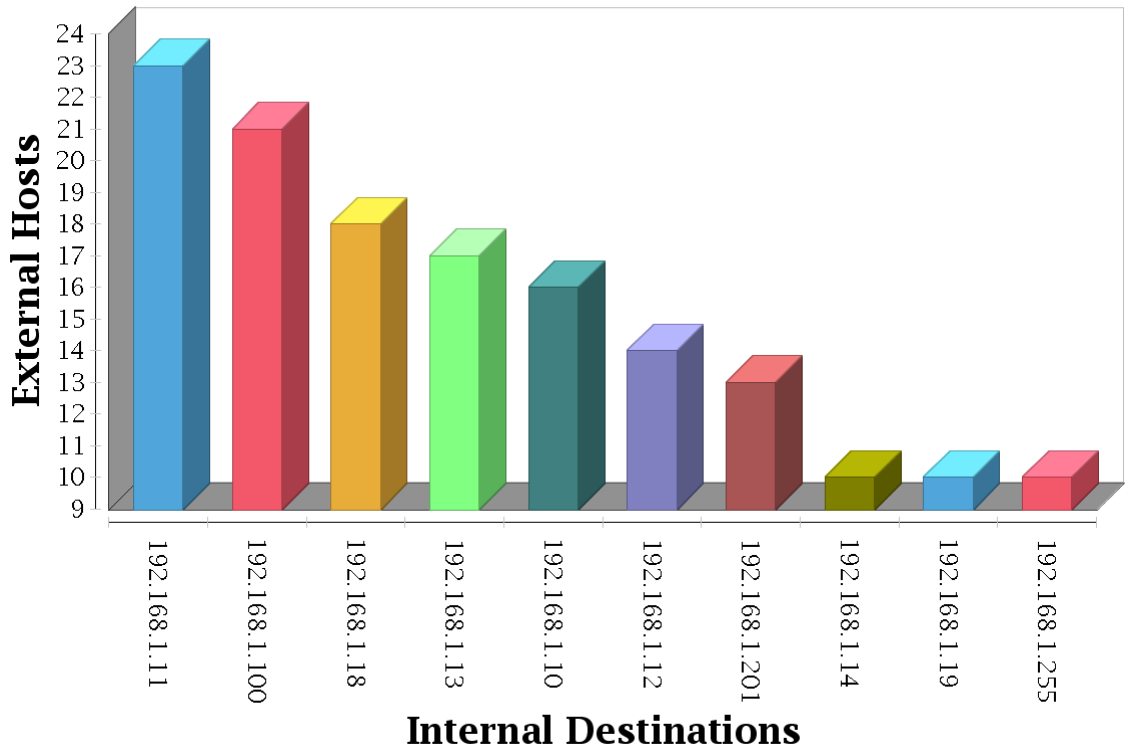
Destination	Destination Hostname	# Internal Hosts	Megs Transferred
192.168.0.11	192.168.0.11	2	3
192.168.0.19	192.168.0.19	4	0
192.168.0.28	192.168.0.28	4	0
192.168.0.15	192.168.0.15	4	0
192.168.0.29	192.168.0.29	5	0
192.168.186.1	192.168.186.1	2	0
192.168.59.1	192.168.59.1	2	0
224.0.1.22	SVRLOC.MCAST.NET	1	0
128.8.10.90	d.root-servers.net	1	0
192.168.0.21	192.168.0.21	2	0

Top Sources of Outgoing Connections



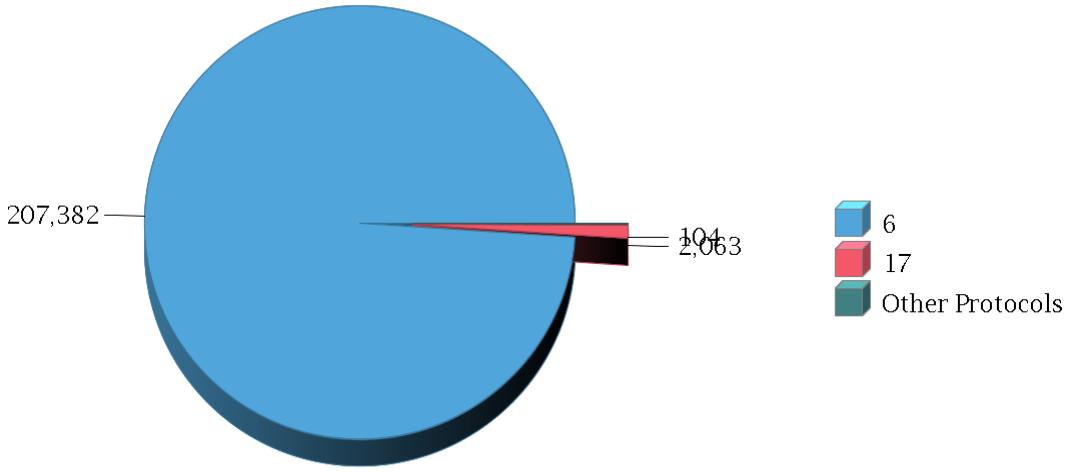
Source	Source Hostname	# External Hosts	Megs Transferred
192.168.1.100	192.168.1.100	22	0
192.168.1.17	192.168.1.17	14	0
192.168.1.201	192.168.1.201	9	0
192.168.1.11	192.168.1.11	6	3
192.168.1.12	192.168.1.12	4	0
192.168.1.200	192.168.1.200	4	0
192.168.1.18	192.168.1.18	3	0
192.168.1.13	192.168.1.13	2	0
192.168.1.16	192.168.1.16	2	0
192.168.1.31	192.168.1.31	2	0

Top Destinations of Incoming Connections

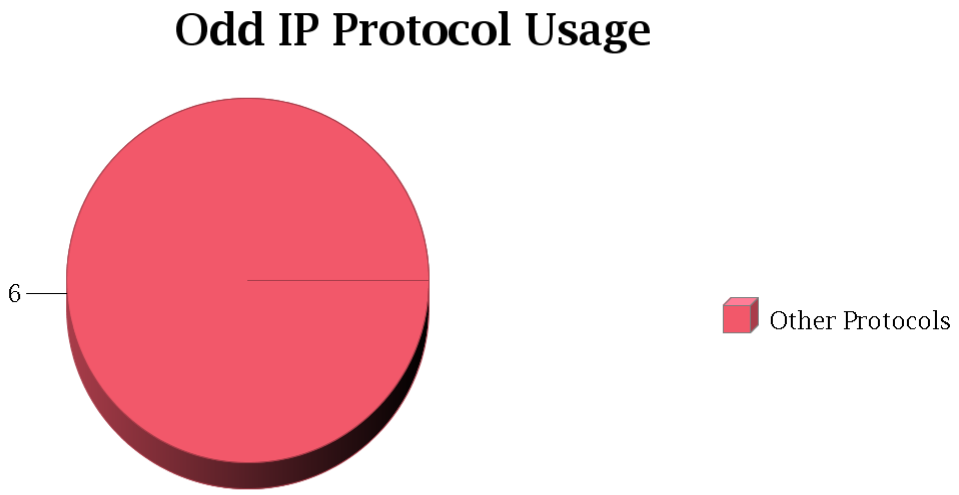


Destination	Destination Hostname	# Sources	Megs Transferred
192.168.1.11	192.168.1.11	23	306
192.168.1.100	192.168.1.100	21	0
192.168.1.18	192.168.1.18	18	4
192.168.1.13	192.168.1.13	17	0
192.168.1.10	192.168.1.10	16	0
192.168.1.12	192.168.1.12	14	1
192.168.1.201	192.168.1.201	13	1
192.168.1.14	192.168.1.14	10	4
192.168.1.19	192.168.1.19	10	0
192.168.1.255	192.168.1.255	10	0

Network Protocol Breakdown



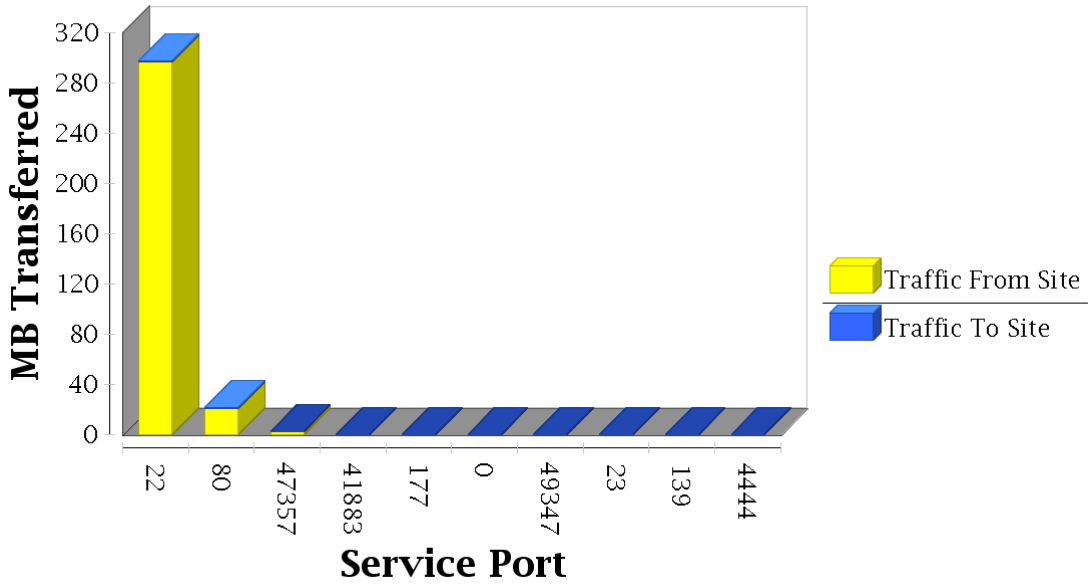
Odd IP Protocol Breakdown



Sessions Inolving Odd IP Protocols

Source	Source Hostname	Destination	Destination Hostname	IP Protocol	Source Bytes	Dest Bytes
192.168.0.14	192.168.0.14	224.0.0.251	224.0.0.251	2	32	0
192.168.0.21	192.168.0.21	224.0.0.251	224.0.0.251	2	24	0
192.168.1.1	192.168.1.1	224.0.0.22	IGMP.MCAST.NET	2	64	0
192.168.1.201	192.168.1.201	224.0.0.22	IGMP.MCAST.NET	2	32	0
192.168.2.1	192.168.2.1	224.0.0.251	224.0.0.251	2	16	0

Most Active Internet Service Ports



Destination Port	Megs To Site	Megs From Site	Total Megs
22	1	297	298
80	1	21	22
47357	0	3	3
41883	0	0	0
177	0	0	0
0	0	0	0
49347	0	0	0
23	0	0	0
139	0	0	0
4444	0	0	0