Global Information Assurance Certification Paper

*** David presents some interesting patterns. Detect 9 is fun reading, since I'm always at work, guess I can't go there.
76 *

Hi,

It's David Nolan.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	19	11:31:49	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:50	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:51	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:58	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:31:59	for	tcp:good.guys.9-80	from	146.82.152.9	9980 Scan	80
Apr	19	11:32:00	for	tcp:good.guys.19-9980	from	146.82.152.9	9980 Scan	9980
Apr	19	11:33:30	for	tcp:good.guys.19-9980	from	146.82.152.9	9980 Scan	9980

I'm calling this the 9980 scan. It is not terribly quick, and it follows this patter in other scans as well. I couldn't find the info for this site, I get a destination unreachable. There is no other traffic from this host, so I'm chalking it up as some kind of portscan.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	15	21:22:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:23:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:24:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:24:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:25:41	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:26:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:26:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:27:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:28:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:28:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:29:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:30:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:30:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:31:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:32:28	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:32:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:33:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:34:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:35:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:36:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:37:42	for	tcp:good.guys.9-80	from	24.0.146.115	Home.com/Roadrunner/PSI	80
Apr	15	21:38:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:40:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980
Apr	15	21:42:41	for	tcp:good.guys.19-9980	from	24.0.146.115	Home.com/Roadrunner/PSI	9980

This is another variation of the '9980 scan'. This time it comes from a user at home.com. Again, we see a slow timestamp, and the same pattern of port 80 to .9 and port 9980 to .19. An odd portscan.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	12	0:29:11	for	tcp:good.guys.2-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:11	for	tcp:good.guys.3-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:15	for	tcp:good.guys.10-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:15	for	tcp:good.guys.6-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:15	for	tcp:good.guys.8-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:15	for	tcp:good.guys.9-1243	from	209.13.228.40	SubSeven Scan	1243
Apr	12	0:29:18	for	tcp:good.guys.2-3264	from	209.13.228.40	Another Trojan Scan?	3264
Apr	12	0:29:18	for	tcp:good.guys.3-3264	from	209.13.228.40	Another Trojan Scan?	3264
Apr	12	0:29:18	for	tcp:good.guys.9-3264	from	209.13.228.40	Another Trojan Scan?	3264
Apr	12	0:29:19	for	tcp:good.guys.9-3264	from	209.13.228.40	Another Trojan Scan?	3264
Apr	12	0:29:20	for	tcp:good.guys.9-3264	from	209.13.228.40	Another Trojan Scan?	3264
Apr	12	0:29:21	for	tcp:good.guys.9-3264	from	209.13.228.40	Another Trojan Scan?	3264

This is a basic sub7 scan with an extra scan to port 3264. It's pretty quick. The address belongs to a host from a ISP-type company in Argentina. I couldn't really decipher the web site, as the english link didn't work. The trace has been edited for brevity. There was no other traffic from this host, so I guess they just moved on. Another port scan.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	4	18:23:51	for	udp:good.guys.10-161	from	12.72.202.181	SNMP Scan	161
Apr	4	18:23:51	for	udp:good.guys.2-161	from	12.72.202.181	SNMP Scan	161
Apr	4	18:23:51	for	udp:good.guys.3-161	from	12.72.202.181	SNMP Scan	161
Apr	4	18:23:51	for	udp:good.guys.4-161	from	12.72.202.181	SNMP Scan	161
Apr	4	18:23:51	for	udp:good.guys.5-161	from	12.72.202.181	SNMP Scan	161
Apr	4	18:23:51	for	udp:good.guys.6-161	from	12.72.202.181	SNMP Scan	161

```
Apr     4       18:23:51        for     udp:good.guys.7-161     from    12.72.202.181   SNMP Scan       161
Apr     4       18:23:51        for     udp:good.guys.8-161     from    12.72.202.181   SNMP Scan       161
Apr     4       18:23:51        for     udp:good.guys.9-161     from    12.72.202.181   SNMP Scan       161
```

This scan came in from a dialup user in Phoenix, Arizona on att.net. I didn't see any other traffic from this address, so I'm guessing the user tried "public" and that's about it.

```
Month   Day     Time            Way     Address                 Way     Address         Possible Detect Port
Apr     12      12:30:39        for     udp:good.guys.10-161    from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.19-161    from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.2-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.3-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.4-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.5-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.6-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.7-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.8-161     from    208.148.52.60   SNMP Scan       161
Apr     12      12:30:39        for     udp:good.guys.9-161     from    208.148.52.60   SNMP Scan       161
```

This SNMP scan came in from a node off of the westelcom.com network. They offer DSL, and it looks like a node on their DSL network from the name. I'm guessing from the tight time signatures, that this was another user testing "public". Another host scan.

```
Month   Day     Time    Way     Address                 Way     Address         Possible Detect         Port
Mar     31      1:08:44 for     tcp:good.guys.2-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.3-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.4-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.5-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.6-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.7-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.8-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.9-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.10-27374  from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.3-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.2-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.8-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.10-27374  from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.7-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.5-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.9-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.6-27374   from    12.75.147.219   SubSeven PortScan       27374
Mar     31      1:08:44 for     tcp:good.guys.4-27374   from    12.75.147.219   SubSeven PortScan       27374
```

Another user from att.net, this time dialing in from Kansas City, MO. It's a pretty quick scan, so I imagine that this was a pretty massive sub7 scan, or at least a scanner that didn't care about being noticed.

In the next section, I group three LinuxConf Scans together, but discuss their attackers separately.

```
Month   Day     Time            Way     Address                 Way     Address         Possible Detect Port
Apr     19      8:06:36         for     tcp:good.guys.2-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.3-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.5-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.7-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.10-98     from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.4-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.6-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.8-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.9-98      from    202.45.48.86    LinuxConf Scan  98
Apr     19      8:06:36         for     tcp:good.guys.19-98     from    202.45.48.86    LinuxConf Scan  98

Apr     20      10:09:56        for     tcp:good.guys.3-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.5-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.7-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.9-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.2-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.4-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.6-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:56        for     tcp:good.guys.19-98     from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.2-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.6-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.7-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.8-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.9-98      from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.10-98     from    203.77.125.54   LinuxConf Scan  98
Apr     20      10:09:59        for     tcp:good.guys.19-98     from    203.77.125.54   LinuxConf Scan  98

Apr     17      9:55:59         for     tcp:good.guys.10-98     from    210.77.145.60   LinuxConf Scan  98
Apr     17      9:55:59         for     tcp:good.guys.19-98     from    210.77.145.60   LinuxConf Scan  98
Apr     17      9:56:02         for     tcp:good.guys.2-98      from    210.77.145.60   LinuxConf Scan  98
Apr     17      9:56:02         for     tcp:good.guys.3-98      from    210.77.145.60   LinuxConf Scan  98
```

Apr	17	9:56:02	for	tcp:good.guys.4-98	from	210.77.145.60	LinuxConf Scan	98	
Apr	17	9:56:02	for	tcp:good.guys.5-98	from	210.77.145.60	LinuxConf Scan	98	
Apr	17	9:56:02	for	tcp:good.guys.6-98	from	210.77.145.60	LinuxConf Scan	98	
Apr	17	9:56:02	for	tcp:good.guys.7-98	from	210.77.145.60	LinuxConf Scan	98	
Apr	17	9:56:02	for	tcp:good.guys.8-98	from	210.77.145.60	LinuxConf Scan	98	
Apr	17	9:56:02	for	tcp:good.guys.9-98	from	210.77.145.60	LinuxConf Scan	98	

All three detects are host scans for a machine running LinuxConf. The timestamps are all tight, and they go to each host on our subnet.

The first address comes to us from the Hong Kong institute of Education. Hmm.

The second address comes to us from a host in the gcn.net.tw domain in Taiwan.

The third remains a mystery to me.

All of these were pretty basic LinuxConf scans. Fortunately, there is nothing for them to find.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Mar	30	20:06:30	for	tcp:good.guys.2-1080	from	4.54.81.177	Ring0	1080
Mar	30	20:06:32	for	tcp:good.guys.2-1080	from	4.54.81.177	Ring0	1080
Mar	30	20:06:33	for	tcp:good.guys.2-1080	from	4.54.81.177	Ring0	1080
Mar	30	20:06:34	for	tcp:good.guys.2-1080	from	4.54.81.177	Ring0	1080
Mar	30	20:30:05	for	tcp:good.guys.2-3128	from	4.54.81.177	Ring0	3128
Mar	30	20:30:06	for	tcp:good.guys.2-3128	from	4.54.81.177	Ring0	3128
Mar	30	20:30:07	for	tcp:good.guys.2-3128	from	4.54.81.177	Ring0	3128
Mar	30	20:30:08	for	tcp:good.guys.2-3128	from	4.54.81.177	Ring0	3128
Mar	30	20:34:56	for	tcp:good.guys.2-8080	from	4.54.81.177	Ring0	8080
Mar	30	20:34:57	for	tcp:good.guys.2-8080	from	4.54.81.177	Ring0	8080
Mar	30	20:34:58	for	tcp:good.guys.2-8080	from	4.54.81.177	Ring0	8080
Mar	30	20:34:59	for	tcp:good.guys.2-8080	from	4.54.81.177	Ring0	8080
Mar	30	21:05:13	for	tcp:good.guys.2-80	from	4.54.81.177	Ring0	80
Mar	30	21:05:14	for	tcp:good.guys.2-80	from	4.54.81.177	Ring0	80
Mar	30	21:05:15	for	tcp:good.guys.2-80	from	4.54.81.177	Ring0	80
Mar	30	21:05:16	for	tcp:good.guys.2-80	from	4.54.81.177	Ring0	80

This is a variant on the original Ring0 scan, as you can note the addition of port 1080 to the list of ports scanned. This came from a dial-up node at bbn.com. Oh well, if it was a permanent IP, I could have told them they were infected. A pretty easy to detect port scan.

Here are two Sun RPC detects.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Mar	31	8:30:29	for	tcp:good.guys.2-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.3-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.4-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.5-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.6-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.7-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.8-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.9-111	from	216.160.126.17	Sun RPC Scan	111
Mar	31	8:30:29	for	tcp:good.guys.10-111	from	216.160.126.17	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.10-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.2-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.3-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.4-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.5-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.6-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.7-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.8-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:53	for	tcp:good.guys.9-111	from	216.160.146.60	Sun RPC Scan	111
Apr	15	6:06:58	for	tcp:good.guys.19-111	from	216.160.146.60	Sun RPC Scan	111

Both scans have quick time stamps, so they either come from a massive scan, or someone who doesn't care about being detected, or both.

The first scan comes from a host called juliet.datacurrent.com. The do web design and hosting. They might have been compromised. Regardless, this was a quick scan.

The second comes from mht-inc.com. That's all I can find about them.

Anyway, these were two standard Sun RPC scans. No other traffic came from these hosts, as all the traffic was denied.

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	19	21:05:28	for	tcp:good.guys.2-53	from	208.180.41.193	DNS Scan	53
Apr	19	21:05:28	for	tcp:good.guys.3-53	from	208.180.41.193	DNS Scan	53
Apr	19	21:05:28	for	tcp:good.guys.4-53	from	208.180.41.193	DNS Scan	53
Apr	19	21:05:28	for	tcp:good.guys.5-53	from	208.180.41.193	DNS Scan	53
Apr	19	21:05:28	for	tcp:good.guys.7-53	from	208.180.41.193	DNS Scan	53

```
Apr     19      21:05:28        for     tcp:good.guys.8-53      from    208.180.41.193  DNS Scan        53
Apr     19      21:05:28        for     tcp:good.guys.9-53      from    208.180.41.193  DNS Scan        53
Apr     19      21:05:28        for     tcp:good.guys.10-53     from    208.180.41.193  DNS Scan        53
Apr     19      21:05:28        for     tcp:good.guys.19-53     from    208.180.41.193  DNS Scan        53
Apr     19      21:28:09        for     udp:good.guys.6-53      from    208.180.41.193  DNS Scan        53
```

This DNS scan came from a node at Cox Internet Services, and it looks like a dialup node. A pretty tight scan on the TCP packets, and then the lone udp packet comes in later. No other traffic from this host was recorded. An odd DNS scan.

```
Month   Day     Time    Way     Address                 Way     Address         Possible Detect         Port
Apr     7       1:30:32 for     tcp:good.guys.2-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:32 for     tcp:good.guys.2-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:32 for     tcp:good.guys.3-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:32 for     tcp:good.guys.4-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:32 for     tcp:good.guys.5-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:32 for     tcp:good.guys.2-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:32 for     tcp:good.guys.2-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:32 for     tcp:good.guys.3-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:32 for     tcp:good.guys.4-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:32 for     tcp:good.guys.5-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:32 for     tcp:good.guys.6-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.10-1880   from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.6-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.6-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.7-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.7-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.8-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.8-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.9-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.9-1880    from    24.14.181.235   Home.com/Roadrunner/PSI 1880
Apr     7       1:30:35 for     tcp:good.guys.10-23     from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.10-23     from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.7-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.7-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.8-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.8-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.9-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
Apr     7       1:30:35 for     tcp:good.guys.9-23      from    24.14.181.235   Home.com/Roadrunner/PSI 23
```

This scan comes to us from another user at home.com. It has been edited for brevity, but 72 packets were received in 3 seconds. We can see that the scan is to all hosts on my subnet, probing telnet and port 1880. I don't know what the second port is for, but I bet it's not good. Anyway, I saw no other traffic from this host, and all packets were blocked. A funky host/port scan.

These last two detects are my favorites, and the most interesting.

This detect is from the 212.108.4 subnet. As many people have posted detects on this, I thought I would summarize the traffic I've seen from it, and give the background information that I have found so far.

The detects look like this:

```
Month   Day     Time    Way     Address                 Way     Address         Possible Detect                 Port
Apr     14      0:56:17 for     tcp:good.guys.2-38139   from    212.108.4.152   High TCP from Porn site.        38139
Apr     17      2:30:16 for     tcp:good.guys.6-41274   from    212.108.4.152   High TCP from Porn site.        41274
Apr     12      3:00:07 for     tcp:good.guys.4-27746   from    212.108.4.152   High TCP from Porn site.        27746
Apr     14      3:12:26 for     tcp:good.guys.4-38652   from    212.108.4.152   High TCP from Porn site.        38652
Apr     19      3:44:34 for     tcp:good.guys.10-32857  from    212.108.4.152   High TCP from Porn site.        32857
Apr     17      4:08:57 for     tcp:good.guys.9-16901   from    212.108.4.152   High TCP from Porn site.        16901
Apr     19      4:40:06 for     tcp:good.guys.3-33036   from    212.108.4.152   High TCP from Porn site.        33036
Apr     13      6:34:39 for     tcp:good.guys.9-37434   from    212.108.4.152   High TCP from Porn site.        37434
Apr     17      7:59:51 for     tcp:good.guys.19-9750   from    212.108.4.152   High TCP from Porn site.        9750
```

The traffic spans from the 4th of April through today (the 21st). It comes from five IP addresses, with the number of packets from each address following the address:

```
212.108.4.152   20
212.108.4.153   11
212.108.4.154   17
212.108.4.178   3
212.108.4.180   7
```

So 58 packets over 17 days isn't a lot, but the traffic looks weird. The place that it comes from is even weirder.
212.108.4.152 is the IP for a server at camsathome.com
212.108.4.153 gives an error page when it's address is put in, so I'm guessing it is a registered user server.
212.108.4.178 is the IP for the main page of www.amsterdamlivexxx.com, don't go there while you are at work.
212.108.4.180 is the IP for the main page of www.camsathome.com, again, don't go there while you are at work.

The result is that all of these sites are hosted by www.interclimax.com, a dutch adult web hosting and design firm. Right now, I have a sniffer trace running to catch any and all packets that come from there from now on. I want to take a look at the captured packets, and then I plan to have a talk with the good people at interclimax.com.

P.S. please don't think I'm a porn freak for finding this. I just happened to telnet to one of the IP's on port 80, and I

found a IIS4.0 web server running. It went from there. Interesting find, though.

This last detect (yeah! finally!) is what I like to call the Oklahoma state scan. It comes from a machine named dms.av.okstate.edu. The scan included 256 packets all received in less than one second. It went to ports 110, 21, 23, 25, 512, 5556, 79, and 80. Most of the hits were to port 80, but the interesting thing is that each host got a packet on each port, and then 19 packets on port 80. The machines that were running web servers got connections from the source ip on ports 2770 to 2830, with ports being repeated. No other traffic is seen from this host. What I found interesting was the port selection ftp, telnet, smtp, finger, web, pop3, sun login and then port 5556. Port 5556 is listed as a possible BO port, but I don't think that is a BO scan. I can't find any sun based service that runs on this port.
I have two theories. One is that port 5556 is for some service that runs on a sun platform that I don't know about. The other is that the traditional ports are used to hide the scan for BO. No matter what it is, though, it is a pretty massive scan. Here are part of the detects:

Denied

Month	Day	Time	Way	Address	Way	Address	Possible Detect	Port
Apr	1	0:53:50	for	tcp:good.guys.10-110	from	139.78.52.223	Oklahoma State Scan	110
Apr	1	0:53:50	for	tcp:good.guys.10-23	from	139.78.52.223	Oklahoma State Scan	23
Apr	1	0:53:50	for	tcp:good.guys.10-25	from	139.78.52.223	Oklahoma State Scan	25
Apr	1	0:53:50	for	tcp:good.guys.10-512	from	139.78.52.223	Oklahoma State Scan	512
Apr	1	0:53:50	for	tcp:good.guys.10-5556	from	139.78.52.223	Oklahoma State Scan	5556
Apr	1	0:53:50	for	tcp:good.guys.10-79	from	139.78.52.223	Oklahoma State Scan	79
Apr	1	0:53:50	for	tcp:good.guys.10-80	from	139.78.52.223	Oklahoma State Scan	80
Apr	1	0:53:47	for	tcp:good.guys.2-110	from	139.78.52.223	Oklahoma State Scan	110
Apr	1	0:53:47	for	tcp:good.guys.2-21	from	139.78.52.223	Oklahoma State Scan	21
Apr	1	0:53:50	for	tcp:good.guys.2-23	from	139.78.52.223	Oklahoma State Scan	23
Apr	1	0:53:50	for	tcp:good.guys.2-25	from	139.78.52.223	Oklahoma State Scan	25
Apr	1	0:53:50	for	tcp:good.guys.2-512	from	139.78.52.223	Oklahoma State Scan	512
Apr	1	0:53:50	for	tcp:good.guys.2-5556	from	139.78.52.223	Oklahoma State Scan	5556
Apr	1	0:53:50	for	tcp:good.guys.2-79	from	139.78.52.223	Oklahoma State Scan	79
Apr	1	0:53:47	for	tcp:good.guys.2-80	from	139.78.52.223	Oklahoma State Scan	80

Accepted

Month	Day	Time	Proto	Way	Address Way	Address	
Apr	1	0:53:50	tcp	from	139.78.52.223-2800	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2802	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2801	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2805	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2806	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2807	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2808	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2809	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2810	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2811	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2812	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2813	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2771	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2818	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2819	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2772	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2820	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2821	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2773	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2822	to	good.guys.9-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2774	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2775	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2778	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2779	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2780	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2781	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2782	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2783	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2784	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2785	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2786	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2791	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2792	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2793	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2794	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2795	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2771	to	good.guys.8-80
Apr	1	0:53:50	tcp	from	139.78.52.223-2772	to	good.guys.8-80

Anyway, that was my Oklahoma State scan.

David Nolan

Last Updated: October 23rd, 2017

Upcoming Training

SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 07, 2018	vLive
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced