Hi,

It's David Nolan.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Way Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:49</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

I'm calling this the 9980 scan. It is not terribly quick, and it follows this pattern 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 chalkin it up as some kind of portscan.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Way Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:49</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>11:31:50</td>
<td>for tcp:good.guys.9-80</td>
<td>from 146.82.152.9</td>
<td>9980 Scan</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Way Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:11</td>
<td>for tcp:good.guys.2-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:11</td>
<td>for tcp:good.guys.3-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.10-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.6-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.8-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.9-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.9-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.9-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.9-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>12</td>
<td>0:29:15</td>
<td>for tcp:good.guys.9-1243</td>
<td>from 209.13.228.40</td>
<td>SubSeven Scan</td>
<td>1243</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Way Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>4</td>
<td>18:23:51</td>
<td>for udp:good.guys.2-161</td>
<td>from 12.72.202.181</td>
<td>SNMP Scan</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>4</td>
<td>18:23:51</td>
<td>for udp:good.guys.3-161</td>
<td>from 12.72.202.181</td>
<td>SNMP Scan</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>4</td>
<td>18:23:51</td>
<td>for udp:good.guys.4-161</td>
<td>from 12.72.202.181</td>
<td>SNMP Scan</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>4</td>
<td>18:23:51</td>
<td>for udp:good.guys.5-161</td>
<td>from 12.72.202.181</td>
<td>SNMP Scan</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>4</td>
<td>18:23:51</td>
<td>for udp:good.guys.6-161</td>
<td>from 12.72.202.181</td>
<td>SNMP Scan</td>
<td>161</td>
<td></td>
</tr>
</tbody>
</table>

© SANS Institute 2000 - 2005
Author retains full rights.
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.

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 another user testing "public". Another host scan.

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.

In the next section, I group three LinuxConf Scans together, but discuss their attackers separately.
Anyway, these were two standard Sun RPC scans. No other traffic came from these hosts, as all the traffic was denied.

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.

Mar 30 20:06:30 for tcp:good.guys.2-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.3-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.4-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.5-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.6-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.7-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.8-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.9-1080 from 4.54.81.177 Ring0 1080

Mar 30 20:06:30 for tcp:good.guys.2-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.3-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.4-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.5-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.6-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.7-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.8-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.9-1080 from 4.54.81.177 Ring0 1080

Mar 30 20:06:30 for tcp:good.guys.2-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.3-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.4-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.5-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.6-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.7-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.8-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.9-1080 from 4.54.81.177 Ring0 1080

Mar 30 20:06:30 for tcp:good.guys.2-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.3-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.4-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.5-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.6-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.7-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.8-1080 from 4.54.81.177 Ring0 1080
Mar 30 20:06:30 for tcp:good.guys.9-1080 from 4.54.81.177 Ring0 1080

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 scans.

Mar 31 8:30:29 for tcp:good.guys.2-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.3-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.4-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.5-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.6-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.7-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.8-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.9-2-111 from 216.160.126.17 Sun RPC Scan 111
Mar 31 8:30:29 for tcp:good.guys.10-2-111 from 216.160.126.17 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 scan 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.
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.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
</table>

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:

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

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 camasathome.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.camasathome.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
Anyway, that was my Oklahoma State scan.
## Upcoming Training

<table>
<thead>
<tr>
<th>Training Event</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS London October 2020</td>
<td>London, United Kingdom</td>
<td>Oct 12, 2020 - Oct 17, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS October Singapore 2020 - Live Online</td>
<td>Singapore, Singapore</td>
<td>Oct 12, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Dallas Fall 2020</td>
<td>Dallas, TX</td>
<td>Oct 19, 2020 - Oct 24, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London November 2020</td>
<td>, United Kingdom</td>
<td>Nov 02, 2020 - Nov 07, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS San Diego Fall 2020</td>
<td>San Diego, CA</td>
<td>Nov 16, 2020 - Nov 21, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Frankfurt November 2020</td>
<td>, Germany</td>
<td>Nov 30, 2020 - Dec 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Cyber Defense Initiative 2020</td>
<td>Washington, DC</td>
<td>Dec 14, 2020 - Dec 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>