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</th>
<th>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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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 information for this site, so I get a destination unreachable. There is no other traffic from this host, so I’m chalk it up as some kind of portscan.

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</th>
<th>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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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 website, 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</th>
<th>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>
<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>
<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>
<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>
<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.

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.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

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.
Here are two Sun RPC detects.

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.

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

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.

Here are two Sun RPC detects.

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.

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

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.

Here are two Sun RPC detects.

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.

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

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.
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 then got caught up in the traffic from there. It was addressed to www.interclimax.com, and then the lone udp packet comes in later. No other traffic from this host was recorded. A low DNS scan.

<table>
<thead>
<tr>
<th>Month</th>
<th>Day</th>
<th>Time</th>
<th>Way</th>
<th>Address</th>
<th>Time</th>
<th>Address</th>
<th>Possible Detect</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr</td>
<td>19</td>
<td>21:05:28</td>
<td>tcp://good.guys.8-53</td>
<td>208.180.41.193</td>
<td>DNS Scan</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>21:05:28</td>
<td>tcp://good.guys.9-53</td>
<td>208.180.41.193</td>
<td>DNS Scan</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>21:05:28</td>
<td>tcp://good.guys.10-53</td>
<td>208.180.41.193</td>
<td>DNS Scan</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>21:05:28</td>
<td>tcp://good.guys.19-53</td>
<td>208.180.41.193</td>
<td>DNS Scan</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>19</td>
<td>21:28:09</td>
<td>udp://good.guys.6-53</td>
<td>208.180.41.193</td>
<td>DNS Scan</td>
<td>53</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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>Time</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>
<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>
<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>
<td></td>
</tr>
<tr>
<td>Apr</td>
<td>14</td>
<td>3:12:26</td>
<td>tcp://good.guys.4-36652</td>
<td>212.108.4.152</td>
<td>High TCP from Porn site.</td>
<td>36652</td>
<td></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>
<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>
<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>
<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>
<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>
<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 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.amsterdamlivevxxx.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...
This last detect (yay! 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:

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

Anyway, that was my Oklahoma State scan.

David Nolan
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago 2019</td>
<td>Chicago, IL</td>
<td>Aug 19, 2019 - Aug 24, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Canberra Spring 2019</td>
<td>Canberra, Australia</td>
<td>Sep 02, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo September 2019</td>
<td>Oslo, Norway</td>
<td>Sep 09, 2019 - Sep 14, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2019</td>
<td>Las Vegas, NV</td>
<td>Sep 09, 2019 - Sep 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TX</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2019</td>
<td>London, United Kingdom</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Santa Monica 2019</td>
<td>Santa Monica, CA</td>
<td>Oct 21, 2019 - Oct 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Toronto SEC503</td>
<td>Toronto, ON</td>
<td>Nov 04, 2019 - Nov 09, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Frankfurt December 2019</td>
<td>Frankfurt, Germany</td>
<td>Dec 09, 2019 - Dec 14, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2020</td>
<td>New Orleans, LA</td>
<td>Feb 01, 2020 - Feb 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Norfolk 2020</td>
<td>Norfolk, VA</td>
<td>Mar 16, 2020 - Mar 21, 2020</td>
<td>Live Event</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>