Global Information Assurance Certification Paper

*** Northcutt, 72 *
Detects submitted to SANS by R.J. (Bob) Long, for IDIC Intrusion Detection certification
---

Source: Sanitized and abbreviated Firewall-1 logs from our company's main Internet connection.
Note: Most detects have been abbreviated to show only representative events, except where pattern was interesting.

Detect #1:
Sequential port scan of our complete Class C, firewall, and probably the ISP subnet it's on.
From: CIMAGNET Communication Information Management, Germany (Small German ISP: www.cimag.de [195.145.171.19])
Does not currently respond to ping. Registration for TCP 1524 is ingreslock. Possibly dial-up, or compromised machine.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
28554	08-Apr-00	22:54:17	Internet	drop	1524	195.145.171.21	ISP.SUBNET.OUR.FW	tcp
28560	08-Apr-00	22:54:39	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.0	tcp
28561	08-Apr-00	22:54:39	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.1	tcp
...	...	...	...	...	...	...	...	...
28818	08-Apr-00	22:54:49	Internet	drop	1524	195.145.171.21	OUR.CLASS-C.LEASE.254	tcp

Detect #2:
Semi-sequential imap scan of our complete class C, plus firewall and likely our ISP's subnet.
From Korea Telecom-PUBNET. Note odd stepping countdown order. Possible tool signature? (full record)

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
9421	9-Apr-00	13:56:23	Internet	drop	imap	210.99.10.189	ISP.SUBNET.OUR.FW	tcp
9424	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.12	tcp
9425	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.13	tcp
9426	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.11	tcp
9427	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.10	tcp
9428	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.9	tcp
9429	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.7	tcp
9430	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.8	tcp
9431	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.6	tcp
9432	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.5	tcp
9433	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.4	tcp
9434	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.3	tcp
9435	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.2	tcp
9436	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.1	tcp
9437	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.0	tcp
9438	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.32	tcp
9439	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.31	tcp
9440	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.30	tcp
9441	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.29	tcp
9442	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.27	tcp
9443	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.28	tcp
9444	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.26	tcp
9445	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.25	tcp
9446	9-Apr-00	13:56:30	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.24	tcp

```
9447 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.23    tcp
9448 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.22    tcp
9449 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.21    tcp
9450 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.20    tcp
9451 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.19    tcp
9452 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.18    tcp
9453 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.17    tcp
9454 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.16    tcp
9455 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.15    tcp
9456 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.14    tcp
9457 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.33    tcp
9458 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.38    tcp
9459 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.37    tcp
9460 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.36    tcp
9461 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.35    tcp
9462 9-Apr-00 13:56:30  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.34    tcp
9463 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.76    tcp
9464 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.74    tcp
9465 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.75    tcp
9466 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.73    tcp
9467 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.72    tcp
9468 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.71    tcp
9469 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.70    tcp
9470 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.69    tcp
9471 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.68    tcp
9472 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.67    tcp
9473 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.66    tcp
9474 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.65    tcp
9475 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.64    tcp
9476 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.63    tcp
9477 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.62    tcp
9478 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.61    tcp
9479 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.60    tcp
9480 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.59    tcp
9481 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.58    tcp
9482 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.57    tcp
9483 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.56    tcp
9484 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.55    tcp
9485 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.54    tcp
9486 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.53    tcp
9487 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.52    tcp
9488 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.51    tcp
9489 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.50    tcp
9490 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.49    tcp
9491 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.48    tcp
9492 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.47    tcp
9493 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.46    tcp
9494 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.45    tcp
9495 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.44    tcp
9496 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.43    tcp
```

```
9497 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.42    tcp
9498 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.41    tcp
9499 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.40    tcp
9500 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.39    tcp
9501 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.79    tcp
9502 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.78    tcp
9503 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.77    tcp
9504 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.80    tcp
9505 9-Apr-00 13:56:31  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.81    tcp
9506 9-Apr-00 13:56:32  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.82    tcp
9507 9-Apr-00 13:56:32  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.83    tcp
9508 9-Apr-00 13:56:32  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.84    tcp
9509 9-Apr-00 13:56:32  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.85    tcp
9510 9-Apr-00 13:56:32  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.86    tcp
9511 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.95    tcp
9512 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.94    tcp
9513 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.93    tcp
9514 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.92    tcp
9515 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.91    tcp
9516 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.90    tcp
9517 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.89    tcp
9518 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.88    tcp
9519 9-Apr-00 13:56:33  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.87    tcp
9520 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.105   tcp
9521 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.104   tcp
9522 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.103   tcp
9523 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.102   tcp
9524 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.101   tcp
9525 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.100   tcp
9526 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.99    tcp
9527 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.98    tcp
9528 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.97    tcp
9529 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.96    tcp
9530 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.147   tcp
9531 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.145   tcp
9532 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.146   tcp
9533 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.144   tcp
9534 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.143   tcp
9535 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.142   tcp
9536 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.141   tcp
9537 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.139   tcp
9538 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.140   tcp
9539 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.137   tcp
9540 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.138   tcp
9541 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.136   tcp
9542 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.135   tcp
9543 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.134   tcp
9544 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.133   tcp
9545 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.132   tcp
9546 9-Apr-00 13:56:34  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.131   tcp
```

9547	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.130	tcp
9548	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.129	tcp
9549	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.127	tcp
9550	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.128	tcp
9551	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.126	tcp
9552	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.125	tcp
9553	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.123	tcp
9554	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.124	tcp
9555	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.121	tcp
9556	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.120	tcp
9557	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.122	tcp
9558	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.119	tcp
9559	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.118	tcp
9560	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.115	tcp
9561	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.117	tcp
9562	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.116	tcp
9563	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.114	tcp
9564	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.113	tcp
9565	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.112	tcp
9566	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.111	tcp
9567	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.109	tcp
9568	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.110	tcp
9569	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.107	tcp
9570	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.108	tcp
9571	9-Apr-00	13:56:34	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.106	tcp
9572	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.148	tcp
9573	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.179	tcp
9574	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.178	tcp
9575	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.177	tcp
9576	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.176	tcp
9577	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.174	tcp
9578	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.175	tcp
9579	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.173	tcp
9580	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.172	tcp
9581	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.171	tcp
9582	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.170	tcp
9583	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.169	tcp
9584	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.167	tcp
9585	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.168	tcp
9586	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.165	tcp
9587	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.166	tcp
9588	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.164	tcp
9589	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.163	tcp
9590	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.162	tcp
9591	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.161	tcp
9592	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.160	tcp
9593	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.159	tcp
9594	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.158	tcp
9595	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.157	tcp
9596	9-Apr-00	13:56:35	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.156	tcp

```
9597 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.155   tcp
9598 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.154   tcp
9599 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.153   tcp
9600 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.152   tcp
9601 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.151   tcp
9602 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.150   tcp
9603 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.149   tcp
9604 9-Apr-00 13:56:35  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.180   tcp
9605 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.187   tcp
9606 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.186   tcp
9607 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.185   tcp
9608 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.184   tcp
9609 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.183   tcp
9610 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.182   tcp
9611 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.181   tcp
9612 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.202   tcp
9613 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.201   tcp
9614 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.200   tcp
9615 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.199   tcp
9616 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.198   tcp
9617 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.197   tcp
9618 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.196   tcp
9619 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.195   tcp
9620 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.194   tcp
9621 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.193   tcp
9622 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.192   tcp
9623 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.191   tcp
9624 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.190   tcp
9625 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.189   tcp
9626 9-Apr-00 13:56:36  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.188   tcp
9627 9-Apr-00 13:56:37  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.203   tcp
9628 9-Apr-00 13:56:37  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.206   tcp
9629 9-Apr-00 13:56:37  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.205   tcp
9630 9-Apr-00 13:56:37  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.204   tcp
9631 9-Apr-00 13:56:38  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.207   tcp
9632 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.214   tcp
9633 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.213   tcp
9634 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.212   tcp
9635 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.211   tcp
9636 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.210   tcp
9637 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.208   tcp
9638 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.209   tcp
9639 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.224   tcp
9640 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.223   tcp
9641 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.222   tcp
9642 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.221   tcp
9643 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.219   tcp
9644 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.220   tcp
9645 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.217   tcp
9646 9-Apr-00 13:56:39  Internet  drop  imap        210.99.10.189 OUR.CLASS-C.LEASE.218   tcp
```

9647	9-Apr-00	13:56:39	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.216	tcp
9648	9-Apr-00	13:56:39	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.215	tcp
9649	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.225	tcp
9650	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.238	tcp
9651	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.237	tcp
9652	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.236	tcp
9653	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.235	tcp
9654	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.234	tcp
9655	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.233	tcp
9656	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.232	tcp
9657	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.230	tcp
9658	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.231	tcp
9659	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.229	tcp
9660	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.228	tcp
9661	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.227	tcp
9662	9-Apr-00	13:56:40	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.226	tcp
9663	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.255	tcp
9664	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.254	tcp
9665	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.253	tcp
9666	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.252	tcp
9667	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.251	tcp
9668	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.250	tcp
9669	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.249	tcp
9670	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.248	tcp
9671	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.247	tcp
9672	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.246	tcp
9673	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.245	tcp
9674	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.244	tcp
9675	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.243	tcp
9676	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.242	tcp
9677	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.241	tcp
9678	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.240	tcp
9679	9-Apr-00	13:56:41	Internet	drop	imap	210.99.10.189	OUR.CLASS-C.LEASE.239	tcp

Detect #3:
Some kind of probe? (mapping? fingerprinting? mutant packets? -not enough data captured by firewall to tell)
From the variable intervals (from 1 sec. To 30min.) appears to be over a broad and randomized IP address range.
Then again, some (4) of our IP's were revisited (many are not even active addresses).
Destination ports are all over the ephemeral road. Pinging source yields "Destination host unreachable."
Possibly bounced off an intermediate host? Apparent source: BTinternet dynamic pool, in Britain. (full record)

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto.
24529	15-Apr-00	18:54:30	Internet	drop	51443	195.99.43.46	OUR.CLASS-C.LEASE.112	tcp
25337	15-Apr-00	19:31:10	Internet	drop	46208	195.99.43.46	OUR.CLASS-C.LEASE.89	tcp
26058	15-Apr-00	20:01:14	Internet	drop	27304	195.99.43.46	OUR.CLASS-C.LEASE.37	tcp
26404	15-Apr-00	20:16:37	Internet	drop	22989	195.99.43.46	OUR.CLASS-C.LEASE.24	tcp
26405	15-Apr-00	20:16:38	Internet	drop	34716	195.99.43.46	OUR.CLASS-C.LEASE.110	tcp
27221	15-Apr-00	20:54:10	Internet	drop	46078	195.99.43.46	OUR.CLASS-C.LEASE.22	tcp
27837	15-Apr-00	21:19:12	Internet	drop	21177	195.99.43.46	OUR.CLASS-C.LEASE.69	tcp

```
 28440 15-Apr-00 21:48:39 Internet  drop  19466             195.99.43.46  OUR.CLASS-C.LEASE.76   tcp
 28664 15-Apr-00 21:59:53 Internet  drop  20819             195.99.43.46  OUR.CLASS-C.LEASE.84   tcp
 28824 15-Apr-00 22:07:42 Internet  drop  23180             195.99.43.46  OUR.CLASS-C.LEASE.93   tcp
 29467 15-Apr-00 22:32:48 Internet  drop  60766             195.99.43.46  OUR.CLASS-C.LEASE.94   tcp
 30001 15-Apr-00 22:52:45 Internet  drop  59154             195.99.43.46  OUR.CLASS-C.LEASE.104  tcp
 30085 15-Apr-00 22:55:46 Internet  drop  51070             195.99.43.46  OUR.CLASS-C.LEASE.42   tcp
 30378 15-Apr-00 23:06:19 Internet  drop  23483             195.99.43.46  OUR.CLASS-C.LEASE.109  tcp
 30607 15-Apr-00 23:16:36 Internet  drop  34771             195.99.43.46  OUR.CLASS-C.LEASE.107  tcp
 30660 15-Apr-00 23:18:57 Internet  drop  52590             195.99.43.46  OUR.CLASS-C.LEASE.29   tcp
   254 16-Apr-00  0:11:32 Internet  drop  56102             195.99.43.46  OUR.CLASS-C.LEASE.57   tcp
  1368 16-Apr-00  1:06:11 Internet  drop  13978             195.99.43.46  OUR.CLASS-C.LEASE.37   tcp
  1523 16-Apr-00  1:13:43 Internet  drop  43963             195.99.43.46  OUR.CLASS-C.LEASE.112  tcp
  2324 16-Apr-00  1:53:10 Internet  drop  27920             195.99.43.46  OUR.CLASS-C.LEASE.56   tcp
  2627 16-Apr-00  2:08:27 Internet  drop  35492             195.99.43.46  OUR.CLASS-C.LEASE.26   tcp
  3571 16-Apr-00  2:55:08 Internet  drop  60254             195.99.43.46  OUR.CLASS-C.LEASE.121  tcp
  4115 16-Apr-00  3:22:01 Internet  drop  37579             195.99.43.46  OUR.CLASS-C.LEASE.64   tcp
  4871 16-Apr-00  3:59:40 Internet  drop  26145             195.99.43.46  OUR.CLASS-C.LEASE.87   tcp
  5474 16-Apr-00  4:29:38 Internet  drop  56910             195.99.43.46  OUR.CLASS-C.LEASE.59   tcp
  5588 16-Apr-00  4:35:23 Internet  drop  10785             195.99.43.46  OUR.CLASS-C.LEASE.53   tcp
  6121 16-Apr-00  5:02:14 Internet  drop  37143             195.99.43.46  OUR.CLASS-C.LEASE.64   tcp
  6314 16-Apr-00  5:11:49 Internet  drop  56556             195.99.43.46  OUR.CLASS-C.LEASE.15   tcp
  7401 16-Apr-00  6:05:54 Internet  drop  47213             195.99.43.46  OUR.CLASS-C.LEASE.23   tcp
  9047 16-Apr-00  7:28:05 Internet  drop  11611             195.99.43.46  OUR.CLASS-C.LEASE.69   tcp


Detect #4:
Sequential scan of complete Class C and firewall for proxy port 1080
From TELE2-BACKBONE  Modempools in Norway

  No.  Date      Time     I/F      Action Service           Source         Destination            Proto.
 15483 20-Apr-00 16:13:04 Internet  drop  1080              193.217.227.10 ISP.SUBNET.OUR.FW      tcp
 15495 20-Apr-00 16:13:52 Internet  drop  1080              193.217.227.10 OUR.CLASS-C.LEASE.1    tcp
       ...               ...       ...   ...               ...            ...                    ...
 15780 20-Apr-00 16:16:05 Internet  drop  1080              193.217.227.10 OUR.CLASS-C.LEASE.254  tcp


Detect #5:
Semi-sequential scan of most (201 addr's) of our Class C, but not firewall, using undetermined icmp type.
From Exodus Commun. (NETBLK-EC21-1)

  No.  Date      Time     I/F      Action Service           Source        Destination            Proto.
 17000 20-Apr-00 17:40:56 Internet  drop                    64.28.74.182  OUR.CLASS-C.LEASE.1    icmp
       ...               ...       ...   ...               ...           ...                    ...
 17220 20-Apr-00 17:40:58 Internet  drop                    64.28.74.182  OUR.CLASS-C.LEASE.254  icmp

Note: verbosity of logs increased from this point on.


Detect #6:
Probe of our firewall on common UDP port for Hack 'a Tack trojan. From MobilCom City LINE GmbH Dialpool in Germany.
```

Note source and dest. ports one number different. This is the only traffic seen from/to 213.6.x.x today, and it's destined for firewall. Address currently responds to ping. Source could be either compromised machine or dial-up.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
6804	21-Apr-00	10:01:33	Internet	drop	UDP31789_HackaTack	213.6.174.21	OUR.CLASS-C.LEASE.49	udp	UDP31790_HackaTack
6805	21-Apr-00	10:01:33	Internet	drop	UDP31789_HackaTack	213.6.174.21	OUR.CLASS-C.LEASE.169	udp	UDP31790_HackaTack

Detect #7:
Sequential scan of most (216 addr's) of our Class C (not firewall) on TCP53 (DNS). Responds to ping. Compromised?
From Connected Networks (NETBLK-CONNECTED-CA) in B.C., Canada

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
13439	21-Apr-00	22:08:41	Internet	reject	nameserver	209.53.123.202	OUR.CLASS-C.LEASE.1	tcp	nameserver
...	...	...	...	...	...	...	...	...	...
13655	21-Apr-00	22:08:46	Internet	reject	nameserver	209.53.123.202	OUR.CLASS-C.LEASE.247	tcp	nameserver

Detect #8a:
Scan of our complete Class-C and firewall on Sub-7 2.1 default port. Does not currently respond to ping (weekday).
From TimeWarnerCable-Road-Runner-TAMPA-mcr23d-24-26-82-0-to-84-0 (NETBLK-RRTAMPA82-84.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
10733	21-Apr-00	16:07:32	Internet	drop	27374	24.26.82.129	ISP.SUBNET.OUR.FW	tcp	22812
10734	21-Apr-00	16:07:40	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.0	tcp	27085
10735	21-Apr-00	16:07:40	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.1	tcp	27086
...	...	...	...	...	...	...	...	...	...
10992	21-Apr-00	16:08:09	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.254	tcp	30978
10993	21-Apr-00	16:08:09	Internet	drop	27374	24.26.82.129	OUR.CLASS-C.LEASE.255	tcp	31041

Detect #8b:
Another Sub-7 scan next day from another location, of most of our Class-C (234 addr's) and firewall.
From PSInet (NET-PSINET-B2-5). Address responds to ping. Could be either dial-up or compromised.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
1187	22-Apr-00	3:24:01	Internet	drop	27374	154.5.156.181	ISP.SUBNET.OUR.FW	tcp	1778
1189	22-Apr-00	3:24:16	Internet	drop	27374	154.5.156.181	OUR.CLASS-C.LEASE.21	tcp	2002
...	...	...	...	...	...	...	...	...	...
1422	22-Apr-00	3:24:29	Internet	drop	27374	154.5.156.181	OUR.CLASS-C.LEASE.254	tcp	2236

Detect #9:
DNS scan of most of our class C (216 addr's), not firewall. Address does not currently respond to ping.
From TimeWarnerCable-Road-Runner-Memphis-HUBD-East-104-106 (NETBLK-TWCMEMEAST).

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
3654	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.2	tcp	4813

3655	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.3	tcp	4814
3656	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.1	tcp	4812
3657	22-Apr-00	9:35:38	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.6	tcp	4817
...	...	...	...	...	...	...	...	...	...
3865	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.247	tcp	1385
3866	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.240	tcp	1378
3867	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.241	tcp	1379
3868	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.244	tcp	1382
3869	22-Apr-00	9:35:41	Internet	reject	nameserver	24.95.106.210	OUR.CLASS-C.LEASE.245	tcp	1383

Detect #10:
Sunrpc scan of most of our class C (201 addr's), and firewall.
From Lesjofors AB on TELIANET-BLK in Sweden. Responds to ping. Likely compromised machine, or possibly dial-up.

No.	Date	Time	I/F	Action	Service	Source	Destination	Proto	S_Port
3884	23-Apr-00	11:25:52	Internet	drop	sunrpc	195.198.109.16	ISP.SUBNET.OUR.FW	tcp	3326
3887	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.0	tcp	3548
3888	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.1	tcp	3549
3889	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.9	tcp	3557
3890	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.2	tcp	3550
3891	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.10	tcp	3558
3892	23-Apr-00	11:25:56	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.4	tcp	3552
...	...	...	...	...	...	...	...	...	...
4087	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.249	tcp	3797
4088	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.252	tcp	3800
4089	23-Apr-00	11:26:06	Internet	drop	sunrpc	195.198.109.16	OUR.CLASS-C.LEASE.250	tcp	3798

Last Updated: June 24th, 2018

Upcoming Training

SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
San Antonio 2018 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS Brussels October 2018	Brussels, Belgium	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	Tysons, VA	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, CO	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, Singapore	Oct 15, 2018 - Oct 27, 2018	Live Event
Mentor Session - SEC503	Ankara, Turkey	Oct 31, 2018 - Dec 19, 2018	Mentor
Mentor Session - SEC503	Ballston, VA	Nov 01, 2018 - Dec 06, 2018	Mentor
SANS Dallas Fall 2018	Dallas, TX	Nov 05, 2018 - Nov 10, 2018	Live Event
San Diego Fall 2018 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	vLive
SANS San Diego Fall 2018	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Stockholm 2018	Stockholm, Sweden	Nov 26, 2018 - Dec 01, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZ	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DC	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced