Global Information Assurance Certification Paper

GIAC Certified Intrusion Analyst Practical

- 5 Detects With Analysis
- "Analyze This"
- Evaluate an Attack

Paul Juhasz

Part I: 4 Detects with Analysis

A. General Background:

Three detects were obtained from the GIAC website (http://www.sans.org/giac.htm). One is a sanitized detect from a system on my network.

Severity was calculated using the formula:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

All of these items are on a 5 point scale.

Criticality = 5 is assigned to the most important systems (Firewall, DNS Server, Core Routers, etc.), 1 is assigned to a very old OS such as MS-DOS 3.11

Lethality = 5 is assigned to severe cases in which an attacker can gain root access across the net, 1 is assigned to an attack that is very unlikely to succeed.

System Countermeasures = 5 is assigned to a modern operating system, all patches, etc… 1 is assigned to a system which allows fixed passwords and has not been patched

Network Countermeasures = 5 is assigned to a very restrictive firewall, 1 is given to a very insecure firewall

The result of the severity is classified as follows:

Low – Severity 0 or less
Moderate – Severity 1-2
High – Severity 3-4
Highest – Severity 5 or higher

B. Correlation Information:

When possible, the detects are correlated with a published alerts from GIAC CERT advisories. If no formal advisory could be located to correlate with the data then any other data that could be obtained for correlation was noted.

Sample Detect Data:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:49.784769 212.0.107.107:53 -> MY.NET.1.6:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x301EF5D7   Ack: 0x5D675915   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:49.904566 212.0.107.107:53 -> MY.NET.1.12:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x301EF5D7   Ack: 0x5D675915   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:50.344187 212.0.107.107:53 -> MY.NET.1.34:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x301EF5D7   Ack: 0x5D675915   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:50.504625 212.0.107.107:53 -> MY.NET.1.42:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x301EF5D7   Ack: 0x5D675915   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:50.885816 212.0.107.107:53 -> MY.NET.1.61:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x1DCB19D2   Ack: 0x123655E3   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:01:51.024165 212.0.107.107:53 -> MY.NET.1.68:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x1DCB19D2   Ack: 0x123655E3   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
<…>
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:23:24.661079 212.0.107.107:53 -> MY.NET.254.224:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0xF33BF67   Ack: 0x20246B9C   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:23:24.674747 212.0.107.107:53 -> MY.NET.254.225:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0xF33BF67   Ack: 0x20246B9C   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:23:24.961173 212.0.107.107:53 -> MY.NET.254.240:53
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x7CA57895   Ack: 0x5456D07E   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/10-14:23:25.021392 212.0.107.107:53 -> MY.NET.254.243:53
```

```
TCP TTL:21 TOS:0x0 ID:39426
**SF**** Seq: 0x7CA57895   Ack: 0x5456D07E   Win: 0x404
00 00 00 00 00 00                                  ......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

1. **Source of trace**
   GIAC Website – http://www.sans.org/capsans.snort/index.htm – Sample files OOSche25.

2. **Detect was generated by**
   Snort

3. **Probability the source address was spoofed**
   Low. The large number of apparently crafted packets delivered in such a short period of time likely indicates an attempt at intelligence gathering using a port scanning. It is doubtful that the perpetrator would have masked his own IP address, as he then would not have received the results of his scanning.

4. **Description of attack**
   Large (3100+) number of TCP packets delivered within a relatively short period of time (from 14:01:49 to 14:23:25 – approx. 22 minutes – on 10/10) from IP address:Port 212.0.107.107:53. All packets had the same TTL:21 TOS:0x0 ID:39426, and the Syn/Fin/Ack flags set. The target port matched the suspect source port. The packets came in groups of (on the average) anywhere from 6 to 10 packets having the same SEQ number. The individual packets in each group were targeted at different IP addresses within MY.NET.

5. **Attack mechanism**
   Initial reaction was that this could have been a reaction to some sort of stimulus from MY.NET. However the data contain no outbound traffic from MY.NET to the suspect IP (212.0.107.107), either before or after the packets in question. Another possibility was that this could have been an attempt to flood MY.NET with a Syn Flood, similar to that used by Kevin Mitnick. However the fact that the packets were addressed to different end systems seems to discount this theory.

   Rather, this attack appears to have been an attempt to map MY.NET to determine what systems may be listening for TCP on port 53 (DNS). The systems in MY.NET were sent a series of Syn/Ack packets, with the Fin flag also set. Setting the Fin and Ack flags could be an attempt to trick the firewall into allowing the packets through, in case it is set to statefully detect and protect against a Syn flood from a single IP address. The selection of port 53 (DNS) also could be an attempt to trick the firewall into allowing the packets through (even though DNS uses UDP for most transactions).

   The scan appear to have been unsuccessful. The traces show no other packets traveling into or out of MY.NET until after each respective pattern of packets ended, which suggests that the systems in MY.NET did not respond to the stimuli.

6. **Correlation**
   Similar patterns were detected on other days from other IP address:Port (for example on 10/04 from 128.2.81.133:21 and 63.195.56.20:21, on 10/07 from 163.10.19.34:21, on 11/22 from 139.130.61.206:109). All of these attacks also are characterized by ID:39426. See sample files OOSche20, OOSche24, and OOSche29

   Snort alerts for these time periods both flag the SYN-FIN scans and provide a portscan summary status from the source IP addresses.

7. **Evidence of active targeting**
   Yes. The packets in this attack were directed solely at port 53 across the IP address range of MY.NET. However, not all systems were targeted. Only selected systems on selected third-octets were scanned. (The other attacks mentioned used other Ports.) This could be indicative of preliminary reconnaissance. However, it also could result from an “intelligent” scanner assigning non-consecutive system addresses in an attempt to escape notice.

8. **Severity**

   Low

   (1 + 1) – (3 + 2) = –3

9. **Defense recommendation**

   Ensure that the intrusion detection system is stateful, to issue alerts in these cases.

10. **Multiple choice question:**

```
A large number of SYN-FIN packets to non-consecutive IP addresses could
indicate:
A) An attempt to flood the target systems
B) And attempt to stress the firewall
C) An attempt to scan the network ← Correct Answer
D) Both A & C
```

Sample Detect Data:

```
10/20-08:56:02.253606  [**] Back Orifice [**] 203.114.231.2:1689 -> MY.NET.98.30:31337
10/20-08:56:02.531907  [**] Back Orifice [**] 203.114.231.2:1704 -> MY.NET.98.61:31337
10/20-08:56:02.838936  [**] Back Orifice [**] 203.114.231.2:1716 -> MY.NET.98.81:31337
10/20-08:56:02.894464  [**] Back Orifice [**] 203.114.231.33:1719 ->
MY.NET.98.86:31337
10/20-08:56:03.034529  [**] Back Orifice [**] 203.114.231.33:1725 ->
MY.NET.98.97:31337
10/20-08:56:03.114450  [**] Back Orifice [**] 203.114.231.33:1729 ->
MY.NET.98.104:31337
10/20-08:56:03.123854  [**] Back Orifice [**] 203.114.231.2:1730 ->
MY.NET.98.106:31337
10/20-08:56:03.503903  [**] Back Orifice [**] 203.114.231.33:1747 ->
MY.NET.98.151:31337
10/20-08:56:03.815495  [**] Back Orifice [**] 203.114.231.2:1760 ->
MY.NET.98.193:31337
10/20-08:56:03.985132  [**] Back Orifice [**] 203.114.231.33:1769 ->
MY.NET.98.214:31337
10/20-08:56:04.001653  [**] Back Orifice [**] 203.114.231.33:1771 ->
MY.NET.98.217:31337
10/20-09:08:06.517986  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.8:31337
10/20-09:08:06.543040  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.9:31337
10/20-09:08:06.570678  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.17:31337
10/20-09:08:06.583372  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.16:31337
10/20-09:08:06.599811  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.21:31337
10/20-09:08:06.612533  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.25:31337
10/20-09:08:06.623855  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.20:31337
10/20-09:08:06.632167  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.27:31337
10/20-09:08:06.634965  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.28:31337
10/20-09:08:06.641534  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.30:31337
10/20-09:08:06.677313  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.35:31337
10/20-09:08:06.691023  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.33:31337
10/20-09:08:06.691078  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.39:31337
10/20-09:08:06.754929  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.47:31337
10/20-09:08:06.887565  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.77:31337
10/20-09:08:06.890390  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.78:31337
10/20-09:08:06.891940  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.76:31337
10/20-09:08:06.904432  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.81:31337
10/20-09:08:06.904529  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.82:31337
10/20-09:08:06.948722  [**] Back Orifice [**] 203.148.182.108:21117 ->
```

```
MY.NET.98.87:31337
10/20-09:08:06.987459  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.89:31337
10/20-09:08:07.102298  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.119:31337
10/20-09:08:07.115296  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.115:31337
10/20-09:08:07.121501  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.116:31337
10/20-09:08:07.139209  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.123:31337
10/20-09:08:07.173633  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.130:31337
10/20-09:08:07.187134  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.136:31337
10/20-09:08:07.188044  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.134:31337
10/20-09:08:07.188099  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.129:31337
10/20-09:08:07.240673  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.146:31337
10/20-09:08:07.248238  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.145:31337
10/20-09:08:07.265418  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.151:31337
10/20-09:08:07.281147  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.150:31337
10/20-09:08:07.385603  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.167:31337
10/20-09:08:07.394167  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.173:31337
10/20-09:08:07.488121  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.193:31337
10/20-09:08:07.522085  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.195:31337
10/20-09:08:07.545333  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.203:31337
10/20-09:08:07.552021  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.201:31337
10/20-09:08:07.568826  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.208:31337
10/20-09:08:07.622964  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.209:31337
10/20-09:08:07.749124  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.231:31337
10/20-09:08:07.750713  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.228:31337
10/20-09:08:07.751445  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.233:31337
10/20-09:08:07.760485  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.232:31337
10/20-09:08:07.779688  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.238:31337
10/20-09:08:07.781997  [**] Back Orifice [**] 203.148.182.108:21117 ->
MY.NET.98.239:31337
10/20-09:23:38.482962  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.21:31337
10/20-09:23:38.623189  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.40:31337
10/20-09:23:38.637216  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.42:31337
10/20-09:23:38.648489  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.45:31337
10/20-09:23:38.692526  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.52:31337
```

```
10/20-09:23:38.702595  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.53:31337
10/20-09:23:38.702837  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.54:31337
10/20-09:23:38.983731  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.105:31337
10/20-09:23:39.113464  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.127:31337
10/20-09:23:39.114116  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.123:31337
10/20-09:23:39.141820  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.124:31337
10/20-09:23:39.171817  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.135:31337
10/20-09:23:39.211830  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.146:31337
10/20-09:23:39.220151  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.145:31337
10/20-09:23:39.231375  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.140:31337
10/20-09:23:39.233713  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.142:31337
10/20-09:23:39.266510  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.148:31337
10/20-09:23:39.286337  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.151:31337
10/20-09:23:39.419334  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.162:31337
10/20-09:23:39.484263  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.168:31337
10/20-09:23:39.491220  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.170:31337
10/20-09:23:39.505559  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.174:31337
10/20-09:23:39.511201  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.171:31337
10/20-09:23:39.518412  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.172:31337
10/20-09:23:39.530297  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.183:31337
10/20-09:23:39.553480  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.182:31337
10/20-09:23:39.571389  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.188:31337
10/20-09:23:39.576165  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.189:31337
10/20-09:23:39.642729  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.195:31337
10/20-09:23:39.691693  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.212:31337
10/20-09:23:39.710188  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.218:31337
10/20-09:23:39.718328  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.211:31337
10/20-09:23:39.725626  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.213:31337
10/20-09:23:39.744810  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.223:31337
10/20-09:23:39.752994  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.226:31337
10/20-09:23:39.763357  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.221:31337
10/20-09:23:39.763996  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.229:31337
10/20-09:23:39.770336  [**] Back Orifice [**] 203.148.182.108:1041 ->
```

```
MY.NET.98.231:31337
10/20-09:23:39.795829  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.237:31337
10/20-09:23:39.835740  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.241:31337
10/20-09:23:39.898656  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.248:31337
10/20-09:23:39.904304  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.250:31337
10/20-09:23:39.924387  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.254:31337
10/20-09:33:31.290306  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.34:31337
10/20-09:33:31.332112  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.37:31337
10/20-09:33:31.370774  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.43:31337
10/20-09:33:31.375948  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.46:31337
10/20-09:33:31.462718  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.60:31337
10/20-09:33:31.490641  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.71:31337
10/20-09:33:31.496918  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.73:31337
10/20-09:33:31.555490  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.81:31337
10/20-09:33:31.650355  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.100:31337
10/20-09:33:31.782041  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.127:31337
10/20-09:33:31.798861  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.126:31337
10/20-09:33:31.816216  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.136:31337
10/20-09:33:31.830570  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.132:31337
10/20-09:33:31.841831  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.135:31337
10/20-09:33:32.097328  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.180:31337
10/20-09:33:32.130393  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.192:31337
10/20-09:33:32.161862  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.202:31337
10/20-09:33:32.220341  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.216:31337
10/20-09:33:32.261862  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.225:31337
10/20-09:33:32.386584  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.243:31337
10/20-09:33:32.405098  [**] Back Orifice [**] 203.148.182.108:1041 ->
MY.NET.98.249:31337
10/20-15:35:29.905780  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.9:31337
10/20-15:35:29.905834  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.10:31337
10/20-15:35:29.905888  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.11:31337
10/20-15:35:29.905941  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.12:31337
10/20-15:35:29.985497  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.25:31337
10/20-15:35:29.985551  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.26:31337
10/20-15:35:29.985604  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.27:31337
10/20-15:35:29.985658  [**] Back Orifice [**] 213.43.77.66:31338 -> MY.NET.97.28:31337
10/20-15:35:31.074559  [**] Back Orifice [**] 213.43.77.66:31338 ->
MY.NET.97.199:31337
10/20-15:35:31.122089  [**] Back Orifice [**] 213.43.77.66:31338 ->
MY.NET.97.207:31337
```

```
10/20-15:35:31.122145  [**] Back Orifice [**] 213.43.77.66:31338 ->
MY.NET.97.208:31337
10/20-15:35:31.122201  [**] Back Orifice [**] 213.43.77.66:31338 ->
MY.NET.97.209:31337
```

1. **Source of trace**
   GIAC Website – http://www.sans.org/capsans.snort/index.htm – Sample file SnortA31

2. **Detect was generated by**
   Snort

3. **Probability the source address was spoofed**
   Low. If the source address was spoofed, the initiator would not know if he succeeded in finding a Back Orifice installation.

4. **Description of attack**
   Source IP issues a series of packets scanning selected systems on MY.NET, to determine if Back Orifice is installed on any of the target systems. MY.NET systems are all targeted on port 31337, the well-known Back Orifice port.

5. **Attack mechanism**
   Snort detected a rapid number of scanning packets on 10/20 between 08:56 and 09:33, in clusters varying in size from 10 to 47 packets, and another cluster of packets at 15:35. The time interval between the clusters was anywhere from 10 to 15 minutes, with the exception of the 15:35 cluster. Packets appeared to come from several different source IP addresses.

   This seems to have been three separate scans. The first, at 08:56, appears to be from two separate systems (203.114.231.2 and 203.114.231.33), and each packet utilized a different source port. The second appears to be a more concentrated attack, from 09:08 to 09:33, all from one source IP address (203.148.182.108) but utilizing two source ports (1041, 21117). The third, at 15:35, appeared to come from source IP 213.43.77.66, port 31338, and seems to be unrelated to the earlier two. Each of these three scans targeted a non-consecutive series of systems on MY.NET.

   This appears to have been three separate attempts to troll MY.NET to determine if Back Orifice is installed on systems.

6. **Correlation**
   Analysis of the other sample Snort data shows that scans for the Back Orifice port also occurred on numerous occasions throughout the period covered by the data.

7. **Evidence of active targeting**
   Yes. The first two scans targeted only systems in subnet MY.NET.98, and the third scan targeted only system in subnet MY.NET.97.

8. **Severity**
   Moderate
   (2 + 4) – (3 + 2) = 1

9. **Defense recommendation**
   Ensure that no services are running on port 31337. Because of the obvious targeting, scan the systems to determine if Back Orifice may have been installed.

10. **Multiple choice question:**

```
A Back Orifice scan is characterized by:
A) Target port 31337 ← Correct Answer
B) Source port 31338
C) Non-consecutive target systems
D) Clusters of packets with spacing intervals
```

Sample Detect Data:

```
10/01-06:17:23.004770  [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3746 -> MY.NET.205.94:21
10/01-06:17:25.604955  [**] site exec - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3739 -> MY.NET.97.206:21
10/01-07:38:44.859097  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3815 -> MY.NET.99.130:21
10/01-07:38:51.118666  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3816 -> MY.NET.130.81:21
10/01-07:38:55.557580  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3818 -> MY.NET.130.242:21
10/01-07:38:58.590607  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3818 -> MY.NET.130.242:21
10/01-07:38:59.756346  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3818 -> MY.NET.130.242:21
10/01-07:46:18.953717  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3820 -> MY.NET.205.94:21
10/01-07:46:19.967002  [**] SITE EXEC - Possible wu-ftpd exploit - GIAC000623 [**]
208.61.44.215:3820 -> MY.NET.205.94:21
```

1. **Source of trace:**
   GIAC Website – http://www.sans.org/capsans.snort/index.htm – Sample file SnortA8

2. **Detect was generated by:**
   Snort

3. **Probability the source address was spoofed:**
   Unknown. However, if this truly was a wu-ftpd exploit, then it is likely that the IP address was spoofed, to cover the perpetrator's tracks.

4. **Description of attack:**
   A single IP address, 208.61.44.215, with varying ports, attempts to connect to port 21 on several IP addresses on MY.NET. Three separate attempts are made on 10/01. The first, at 06:17, targets addresses MY.NET.205.94 and MY.NET.97.206 once each. The second, at 07:38, targets MY.NET.99.130 and MY.NET.130.81 once each, and MY.NET.130.242 three times. The last, at 07:46, again targets MY.NET.205.94, this time twice.

5. **Attack mechanism:**
   As described in the correlation references, this exposure has the potential of compromising the target systems and granting root access. This can be accomplished by generating a MAPPING_CHDIR or Message file buffer overflow, or by generating a memory consumption problem in the FTP server.

6. **Correlation:**
   CERT® Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTPD
   CIAC Informatory Bulletin J-065: Wu-ftpd Vulnerability (from The WU-FTPD Development Group)

7. **Evidence of active targeting:**
   Yes, this seems to have targeted a limited number of hosts, with repeated attempts made against two specific hosts, MY.NET.130.242 and MY.NET.205.94.

8. **Severity:**
   High
   (4 + 5) – (1 + 1) = 7

9. **Defense recommendation:**

The correlation references should be read. Verify whether the ftp daemon on the systems in question is an affected wu-ftpd release (wu-ftpd 2.4.2) or a derivative. Take appropriate measures to ensure that ftpd is upgraded to a version in which the exposure has been closed (wu-ftpd 2.5.0 with patches, or later).

10. Multiple choice question:

```
The wu-ftpd exposure affects:
A) All versions of FTP
B) Wu-ftpd and its derivatives <- Correct Answer
C) Only wu-ftpd 2.4.0
D) All releases of wu-ftpd
```

Sample Detect Data:

1. **Source of trace:**
   Solaris system log *messages* file.

2. **Detect generated by:**
   Big Brother system monitor, from the MacLawran group. It is available at www.bb4.com for download.

3. **Probability the source address was spoofed:**
   Not applicable, as this is not a network detect but, rather, a detected anomaly in system activity.

4. **Description of attack:**
   The Big Brother system monitor detected and reported the following messages in the messages file of a Solaris-based intrusion detection system. The messages were issued on system *sysname* within less than two minutes of each other. The sanitized portions of the messages are italicized:

   mmm dd 18:31:10 *sysname* unix: NOTICE: pcfs: illegal disk file format
   mmm dd 18:32:20 *sysname* unix: NOTICE: pcfs: illegal disk file format

5. **Attack Mechanism:**
   Our Big Brother system monitor alerted us flagging the message as a Warning message, based on the unix-determined severity of the message. Review of the system verified that the system message file contained the messages.

   The messages were particularly unusual and disturbing because:
   - The messages were issued outside of normal working hours for the site. The time of the incident was at approximately 18:30 GMT. Moreover, the day of the incident was a Federal Holiday.
   - The system is a critical part of the network IDS infrastructure.
   - The IDS software is installed over a core (minimal) installation of the Solaris operating system. No software is supposed to be operational except for that necessary to perform IDS functions.
   - The system in question is in a location with good physical security controls.
   - The system operates in a relatively hands-off mode. No-one should be accessing the system, except for System Administrators when maintenance needs to be performed.

   These combined issues raised the concern that someone might have been attempting to access data or configuration information on the IDS system.

6. **Correlation:**
   I contacted the on-duty SA by telephone. He had no knowledge of anyone accessing the system, and confirmed that no-one was supposed to be there on that holiday. He then checked several access logs, including the log of room access. This confirmed that a lead SA had been in the data center that day, at a time spanning the detected incident. A check confirmed that the lead SA had accessed the system at the specified times.

   It was determined that the lead SA had been accessing the system in order to extract IDS configuration information in preparation for installing another IDS system, which was to be configured similar to *sysname*, and inadvertently had used a DOS-formatted diskette.

7. **Evidence of active targeting:**
   Not applicable from a network sense. However, the system was deliberately accessed by the SA.

8. **Severity:**
   Highest

(5 + 2) – (2 + 0) = 5 ***Note:*** No number was assigned to the Network Security component of the equation because network access was not a factor in this incident.

9. Defense recommendation:

This was an anomalous incident, unlikely to recur. Discussion with the on-site SAs confirmed that established system and physical access controls were not circumvented, and that the system was in no danger of compromise.

10. Multiple choice question:

A data analyst should:

A) Use multiple sources of detects.
B) Have a working knowledge of the system(s) he is monitoring.
C) Both A and B. ← Correct Answer
D) None of the above

Part II: Analysis Report

[redacted]

Computer Security Analysis Report:

This analysis report includes the following types of information:

Suspicious Hosts: - Hosts which have created network traffic deemed to be of "non-normal" nature. This includes such traffic as numerous port scans, NMAP related scans, and general reconnaissance.

Compromised Hosts: - Hosts which appear to have been compromised in some form or fashion – if possible the method of compromise will be noted

Common Ports Targeted: - Ports and services which are commonly targeted..

D-Port: - Destination Port, the port on the target host which traffic was directed to – listed only if the port seems to be significant (i.e. low port, known port, etc.)

Note: General problems such as mis-configured hardware or defective hardware could have created the data represented in this section.

Common Ports Targeted:

```
7          -          ECHO
21         -          FTP
23         -          TELNET
53         -          DNS
137        -          NETBIOS
1080       -          Common Wingate / Socks port
31337      -          Back Orifice
```

The following table lists selected detects. They are listed if the source IP, destination IP, or destination port occurred with unusual frequency, or if the detects are particularly significant.

Suspicious Hosts:	Activity:	Destination:	D-Port
Numerous Hosts	Back Orifice	MY.NET.97xx, MY.NET.98.xx	31337
Numerous Hosts	Broadcast Ping	MY.NET.70.255	---
200.191.80.181 , 200.191.80.206	External RPC Call	MY.NET.6.15	111
192.102.197.234	NMAP TCP Ping	MY.NET.1.8	53
	Probable NMAP fingerprint attempt	Numerous Hosts	Numerous
194.159.250.7	Null scan!	MY.NET.227.10	Numerous
205.188.153.xxx	Attempted SUNRPC highport access	MY.NET.225.210, Numerous Hosts	32771
216.10.12.30	Successful SUNRPC highport access	MY.NET.202.242, MY.NET.206.222	32771
Numerous Hosts	WinGate 1080 Attempt	Numerous Hosts	8080
24.3.161.193	Queso fingerprint	MY.NET.145.9	110
64.80.63.121	Queso Fingerprint	Numerous	6345, 6346
212.0.107.107	SYN-FIN scan	Numerous Hosts	53
63.195.56.20	SYN-FIN scan	Numerous Hosts	21
195.103.69.159	SYN-FIN scan	Numerous Hosts	53
Numerous MY.NET.97. and MY.NET.98. hosts	SNMP public access	MY.NET.101.192	161
208.61.44.215	wu-ftpd	Numerous	21

I consider the SYN-FIN scans from 212.0.107.107, 63.195.56.20, and 195.103.69.159 to be fairly serious alerts. These were scans directed to the DNS named server port, and the FTP port, with the SF flags set in an atempt to evade intrusion detection systems. Most likely the perpetrator was trying to find the version of bind to determine if there is a possible exploit. These scans were spread out over a wide span of time.

I also consider the possible wu-ftpd exploit to be very serious, because that exploit presents a danger of root access compromise. It is unclear from the pattern whether the targeted MY.NET systems were merely being scanned, or if they are compromised.

Possible Compromised Host:	Reason:	Method:
MY.NET.101.192	Numerous SNMP Public Accesses	Attackers apparently take advantage of default “public” SNMP community string. This machine is insecure by configuration
MY.NET.221.82, MY.NET.130.242 (and several others)	Possible wu-ftpd exploit	Attackers apparently are attempting to determine if the targeted systems are vulnerable to the wu-ftpd exploit. They actively target FTP port 21.

Overall Analysis:

Network Security:

Overall, this network appears to be relatively secure. There is sufficient evidence to conclude, however, that if an insecure system is put on the network it will quickly be found due to the high amount of scanning being done.

Compromised Systems:

It does appear that there might be at least one compromised system, MY.NET.101.192. Several others may also be compromised by the wu-ftpd exploit.

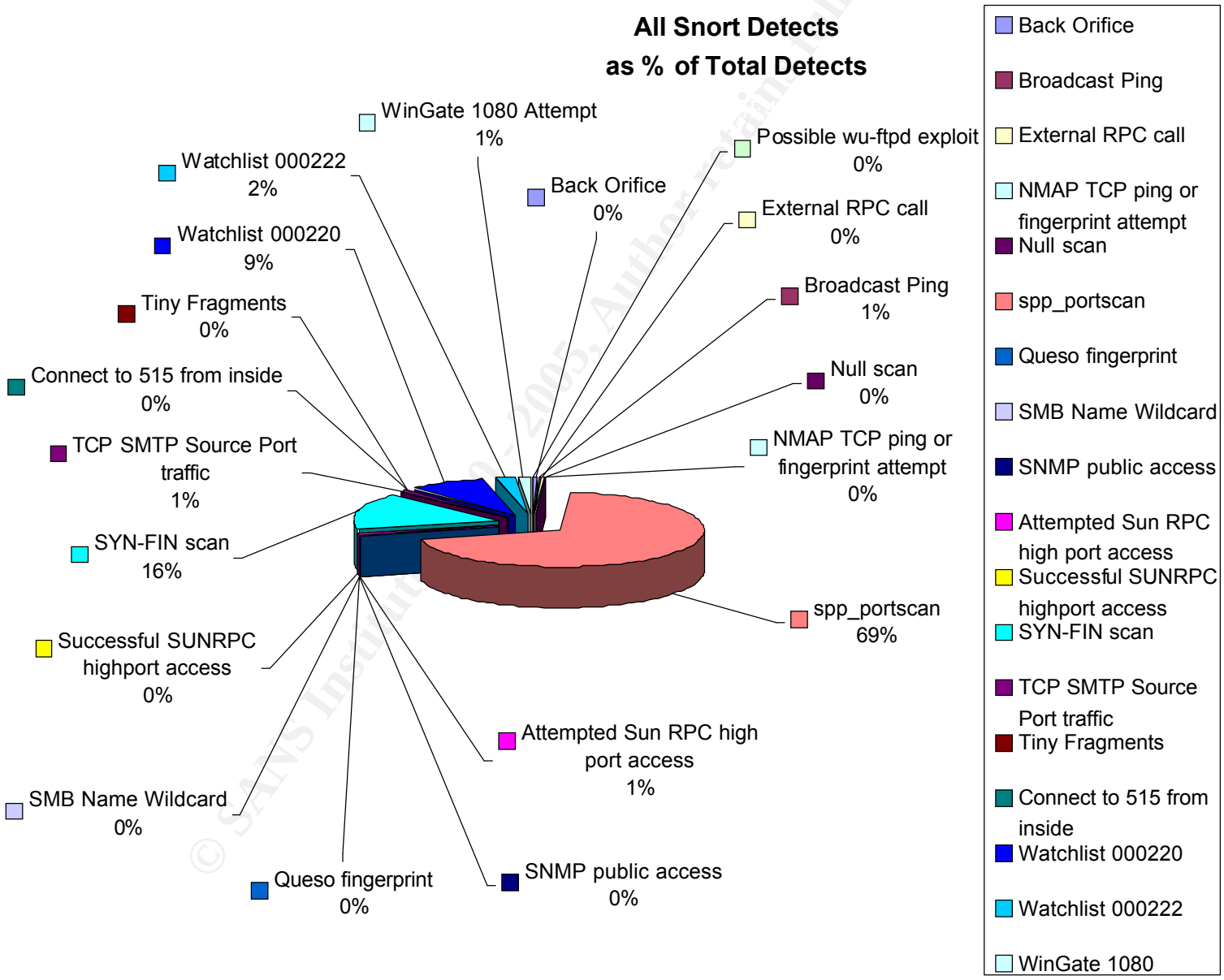
Most serious scanned services: DNS and FTP - Most serious of the ones that were scanned frequently.

Note also that there are large gaps of time in the data, where there are no reported alerts – this could be caused to inactive detectors, disk capacity issues, or a strange lapse in attacks. As a lapse in attacks is unlikely, the other possibilities warrant further investigation. These gaps of data would indicate that the actual number of attacks for the time period is rather higher than the number of detects reported.

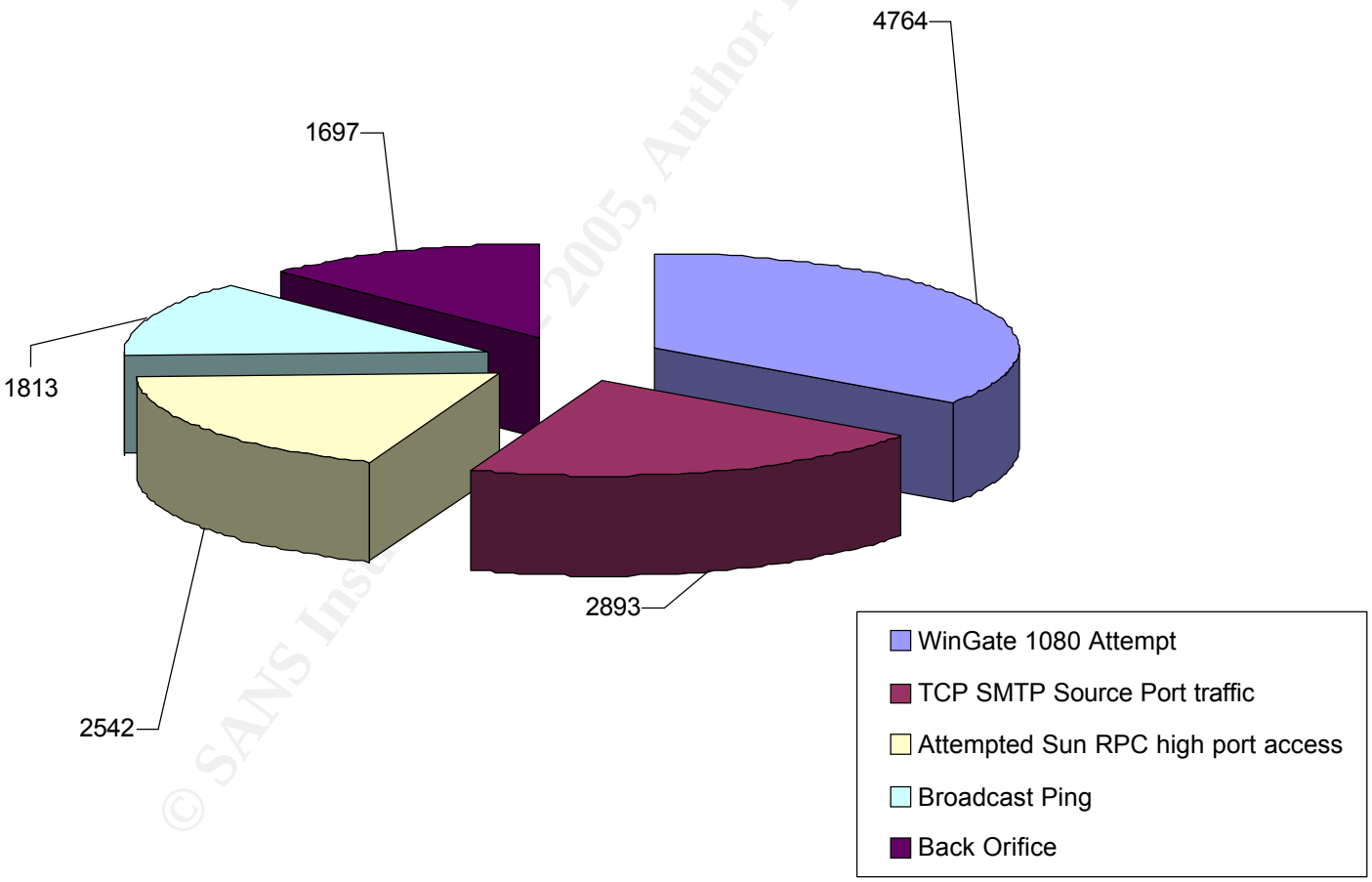
Graphs:
Due to excel limitations (a maximum of 65,536 rows) I decided to use the reduced data as input into the graphs.

The first graph shows the percentage that each detect represented.

To produce the second graph, I decided to leave out the SYN-FIN and portscan detects, and the two flavors of Watchlist detects. The graph shows the number of detects of the top five detects left.



Top Five Detect Types



Part III: Analysis Process

Computer Security Analysis Methodology:

The data which were downloaded from SANS/GIAC web site presented a challenge to my normal analysis techniques. Normally, I would select (or be assigned) a single detect to analyze. This would present a relatively limited amount of data to be considered. By contrast, the data supplied for this Practical Exercise were voluminous. In addition, the data were supplied in numerous files. As a result I decided to take a phased approach to the analysis process.

First step:

After downloading the data from the SANS web page, the first task was to uncompress it to see how much data needed to be analyzed. The respective directories contained for following amount of data:

SnortA	14.9 MB	54 files
SnortS	21.2 MB	42 files
OOS	16.7 MB	19 files

It quickly became obvious that some method for correlating the data would be necessary. I reviewed the contents of the directories and decided that I should treat the directories somewhat differently. I concentrated on the SnortA data for the bulk of my analysis to determine what types of detects Snort flagged. I used the OOS data primarily for the analysis of detect attacks. The SnortS data proved to be primarily SYN data.

Second step:

The next step was to separate the data out into the various types of detects which Snort flagged. Using the data from the SnortA directory, I performed a quick eye-ball scan of several of the files, to determine what the most common entries appeared to be. These proved to be SIN-FIN and portscan entries. I decided that the most straightforward way to break the data into manageable sections would be to reduce the data incrementally into files containing the various alerts.

Third step:

I selected grep as the easiest tool to use for separating out the data. Since I was using a Windows NT system, I downloaded and installed a copy of GNU grep version 2.0b, which was ported to the Win32 environment by Ahmad Abualsamid and Tim Charron.

I first extracted the portscan summary records and the SYN-FIN records into their own text files. I used the following grep commands to extract the data:

```
grep  “End of portscan”  SnortA*.txt  >  portscan.txt
grep  “SYN-FIN”  SnortA*.txt  >  synfin.txt
```

I then culled out the SYN-FIN records and all the portscan records and placed the remainder in a composite file:

```
grep  -v  “portscan”  SnortA*.txt  |  grep  -v  “SYN-FIN”  SnortA*.txt  |  hold.txt
```

I then viewed the hold.txt file and, in turn, extracted and culled out records for the other detects, using the same combination of grep and grep –v commands as above. For example:

```
grep  “Back Orifice”  SnortA*.txt  >  backo.txt
grep  -v  “Back Orifice”  SnortA*.txt  >  hold.txt
```

This step was repeated until no more detect records were left in the hold.txt file. I ended up with a set of 19 text files of varying sizes, each containing one type of detect:

Back Orifice
Broadcast Ping
External RPC call
NMAP TCP ping or fingerprint attempt
Null scan
spp_portscan
Queso fingerprint
SMB Name Wildcard
SNMP public access
Attempted Sun RPC high port access
Successful SUNRPC highport access
SYN-FIN scan
TCP SMTP Source Port traffic
Tiny Fragments
Connect to 515 from inside
Watchlist 000220
Watchlist 000222
WinGate 1080 Attempt
Possible wu-ftpd exploit

Fourth step:

I then began to analyze the data. My goal was first to figure out the relative frequency of the various detects. Since each of the detect entries contains the string "[**]", I was again able to use grep to produce counts of the number of detects recorded of each type. This was done using the grep command:

```
Grep  -c  "[**]"  *.txt  >  counts.txt
```

I also performed the inverse scan to ensure that no records were missed in the count (none were missed):

```
Grep  -c -v  "[**]"  *.txt
```

There was one exception to this rule, however. The extracted portscan summary records contained a count of the total number of hosts scanned during a single detect. For example:

```
10/10-01:32:39.917526  [**] spp_portscan: End of portscan from 24.94.177.249 (TOTAL HOSTS:1 TCP:1 UDP:0) [**]
```

To obtain an accurate count of the total number of portscans performed, I imported the portscan.txt file into MS/Excel, delimited by spaces and colons. I then used a simple Excel formula to provide a summary of the total number of hosts scanned across all the detect entries. I also produced a summary of TCP and UDP scan totals from the same file.

Fifth step:

I then performed triage on the detects, basically making a judgement call of which detects were the most significant and required immediate attention, as opposed to those which could be left for later analysis. Using the data above as a starting point, I performed an initial comparison of the raw data files (SnortA, SnortS, and OOS files) to determine if, for example, the SYN-FIN scans were answered by the internal systems. Some examples of how I categorized the importance of the detects is:

Immediate:	possible wu-ftpd exploit
	successful SUNRPC high port calls
	the Queso fingerprint.
	SNMP public access
Deferred:	Back Orifice
	SYN-FIN

Note: The SYN-FIN detects were deferred for later analysis because, while voluminous and obtrusive, they apparently didn't elicit the expected response from the systems.

Sixth step:

I then reviewed the data in more detail for the detects requiring immediate attention, concentrating on determining the frequency of occurrence of both the source and target IP addresses and ports.

Seventh step:

Finally, using the data extracted in the previous steps, I produced the above charts using MS/Excel.

For further consideration:

As mentioned above, this was a somewhat atypical analysis due to the volume of data submitted for review. In retrospect my analysis techniques could be improved significantly with several enhancements:

- Prepare scripts (perl, shell, etc.) to facilitate sub-setting the data more efficiently into the various types of detects.
- Develop a better methodology for tabulating the number of instances a given IP address (source or target) is involved in a type of detect.
- Prepare a set of statistics, and perhaps charts, showing the dates and times of day of the most frequent attacks.
- Correlate the high-activity source ports with the high-activity target ports.
- Correlate the high-activity source ports with the high-activity target ports.
- Develop a more formal method of performing triage on the data.