Global Information Assurance Certification Paper

*** Northcutt, this might minimally pass, but he scored a 69 on the test *

Thomas Juergensen, Munich, Germany

10 analyzed detects for IDIC 2000

Apr 18, 2000

Note: All IP addresses have been made anonymous. They do not represent real addresses.

Detect example #1:

```
 4Apr2000 10:35:38 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 80 s_port 2464 rule 66
 4Apr2000 10:35:39 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 21 s_port 2465 rule 66
 4Apr2000 10:35:40 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 23 s_port 2466 rule 66
 4Apr2000 10:35:41 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 8080 s_port 2467 rule 66
 4Apr2000 10:35:42 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 3128 s_port 2468 rule 66
 4Apr2000 10:35:43 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 81 s_port 2469 rule 66
 4Apr2000 10:38:28 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 80 s_port 2471 rule 66
 4Apr2000 10:38:29 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 21 s_port 2472 rule 66
 4Apr2000 10:38:30 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 23 s_port 2473 rule 66
 4Apr2000 10:38:31 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 8080 s_port 2474 rule 66
 4Apr2000 10:38:32 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 3128 s_port 2475 rule 66
 4Apr2000 10:38:33 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 81 s_port 2476 rule 66
 4Apr2000 10:38:58 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 80 s_port 2477 rule 66
 4Apr2000 10:38:59 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 21 s_port 2478 rule 66
 4Apr2000 10:39:00 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 23 s_port 2479 rule 66
 4Apr2000 10:39:01 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 8080 s_port 2480 rule 66
 4Apr2000 10:39:02 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 3128 s_port 2481 rule 66
 4Apr2000 10:39:03 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 81 s_port 2482 rule 66
 4Apr2000 10:39:29 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 80 s_port 2483 rule 66
 4Apr2000 10:39:30 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 21 s_port 2484 rule 66
 4Apr2000 10:39:31 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 23 s_port 2485 rule 66
 4Apr2000 10:39:32 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 8080 s_port 2486 rule 66
 4Apr2000 10:39:33 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 3128 s_port 2487 rule 66
 4Apr2000 10:39:34 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 81 s_port 2488 rule 66
 4Apr2000 10:39:49 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 80 s_port 2489 rule 66
 4Apr2000 10:39:50 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 21 s_port 2490 rule 66
 4Apr2000 10:39:51 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 23 s_port 2491 rule 66
 4Apr2000 10:39:52 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 8080 s_port 2492 rule 66
 4Apr2000 10:39:53 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 3128 s_port 2493 rule 66
 4Apr2000 10:39:54 drop 172.33.21.19  <hme0 proto tcp src 192.23.140.34 dst 192.25.140.16 service 81 s_port 2494 rule 66
```

History
- not known

Techniques
- Automated scan: several tries per minute, source port increasing continuously
- TCP scan
- Repeated scan

Intent:
- Scan for open ports: 21 = ftp, 23 = telnet, 80 = http, 81 = http, 8080 = http

Active targeting
- Yes, at least information gathering

Result: Port scan

Detect example #2:

```
 16:31:56.943941 172.25.140.16.1176 > 172.21.131.87.12345: S 228964650:228964650(0) win 8192 <mss 1460> (DF)
 16:31:56.943976 172.21.131.87.12345 > 172.25.140.16.1176: R 0:0(0) ack 228964651 win 0
 16:31:57.433158 172.25.140.16.1176 > 172.21.131.87.12345: S 228964650:228964650(0) win 8192 <mss 1460> (DF)
 16:31:57.433191 172.21.131.87.12345 > 172.25.140.16.1176: R 0:0(0) ack 1 win 0
 16:31:57.933715 172.25.140.16.1176 > 172.21.131.87.12345: S 228964650:228964650(0) win 8192 <mss 1460> (DF)
 16:31:57.933745 172.21.131.87.12345 > 172.25.140.16.1176: R 0:0(0) ack 1 win 0
 16:31:58.434294 172.25.140.16.1176 > 172.21.131.87.12345: S 228964650:228964650(0) win 8192 <mss 1460> (DF)
 16:31:58.434322 172.21.131.87.12345 > 172.25.140.16.1176: R 0:0(0) ack 1 win 0
```

History
- not known

Techniques
- TCP scan
- Repeated scan

Intent:
- Scan for open port: 12345

Active targeting
- Yes

Result: perhaps netbus scan; dest does not listen to port 12345

Detect example #3:

```
 10:01:18.203525 172.23.124.34.1428 > 172.29.204.56.5632: udp 2 10:01:18.203914 172.29.204.56 > 172.23.124.34: icmp: 172.29.204.56 udp port 5632
unreachable 10:01:18.222019 172.23.124.34.1428 > 172.29.204.56.22: udp 2 10:01:18.222594 172.29.204.56 > 172.23.124.34: icmp: 172.29.204.56 udp port 22
unreachable 10:01:18.246441 172.23.124.34.1428 > 172.29.204.125.5632: udp 2 10:01:18.247621 172.29.204.125 > 172.23.124.34: icmp: 172.29.204.125 udp port
5632 unreachable 10:01:18.262401 172.23.124.34.1428 > 172.29.204.125.22: udp 2 10:01:18.263096 172.29.204.125 > 172.23.124.34: icmp: 172.29.204.125 udp
```

```
port 22 unreachable 10:01:18.290194 172.23.124.34.1428 > 139.23.202.6.5632: udp 2 10:01:18.297367 172.23.124.34.1428 > 139.23.202.6.22: udp 2
10:01:18.328231 172.23.124.34.1428 > 172.29.204.126.5632: udp 2 10:01:18.328705 172.29.204.126 > 172.23.124.34: icmp: 172.29.204.126 udp port 5632
unreachable 10:01:18.336714 172.23.124.34.1428 > 172.29.204.126.22: udp 2 10:01:18.337120 172.29.204.126 > 172.23.124.34: icmp: 172.29.204.126 udp port 22
unreachable 10:01:18.346274 172.23.124.34.1428 > 172.29.204.136.5632: udp 2 10:01:18.357046 172.23.124.34.1428 > 172.29.204.136.22: udp 2 10:01:18.386338
172.23.124.34.1428 > 172.29.204.158.5632: udp 2 10:01:18.386978 172.29.204.158 > 172.23.124.34: icmp: 172.29.204.158 udp port 5632 unreachable
10:01:18.396439 172.23.124.34.1428 > 172.29.204.158.22: udp 2 10:01:18.397024 172.29.204.158 > 172.23.124.34: icmp: 172.29.204.158 udp port 22
unreachable
History
- not known

Techniques
- Automated scan: several tries, several dest per second
- UDP scan
- Repeated scan

Intent:
- Scan for open ports: 22, 5623


Active targeting
- Yes

Result: scan for pcANYWHERE-hosts; no hosts found

-------------------------------------------------------------------------------------------------------------------------------
Detect example #4:

 07:12:00.428755 192.129.115.178> 172.128.75.26: icmp: echo request
 07:12:00.428964 192.129.115.178.iad2 > 172.128.75.26.snmp: GetNextRequest(40) system.sysObjectID system.sysDescr
 07:12:18.974024 192.129.115.178> 172.128.75.27: icmp: echo request
 07:12:18.974402 172.128.75.27 > 192.129.115.178: icmp: echo reply
 07:12:18.974689 192.129.115.178.iad2 > 172.128.75.27.snmp: GetNextRequest(40) system.sysObjectID system.sysDescr
 07:12:18.974940 172.128.75.27 > 192.129.115.178: icmp: 172.128.75.27 udp port snmp unreachable [tos 0xc0]
 07:13:13.065276 192.129.115.178> 172.128.75.27: icmp: echo request
 07:13:13.065554 172.128.75.27 > 192.129.115.178: icmp: echo reply
 07:14:04.173837 192.129.115.178.ftrapid-1 > 172.128.75.27.http: S 539762:539762(0) win 8192 <mss 1460> (DF)
 07:14:04.174190 172.128.75.27.http > 192.129.115.178.ftrapid-1: R 0:0(0) ack 539763 win 0
 07:14:04.631577 192.129.115.178.ftrapid-1 > 172.128.75.27.http: S 539762:539762(0) win 8192 <mss 1460> (DF)
 07:14:04.631825 172.128.75.27.http > 192.129.115.178.ftrapid-1: R 0:0(0) ack 1 win 0
 07:14:05.132367 192.129.115.178.ftrapid-1 > 172.128.75.27.http: S 539762:539762(0) win 8192 <mss 1460> (DF)
 07:14:05.132616 172.128.75.27.http > 192.129.115.178.ftrapid-1: R 0:0(0) ack 1 win 0
 07:14:05.630638 192.129.115.178.ftrapid-1 > 172.128.75.27.http: S 539762:539762(0) win 8192 <mss 1460> (DF)
 07:14:05.630890 172.128.75.27.http > 192.129.115.178.ftrapid-1: R 0:0(0) ack 1 win 0
 07:14:05.661082 192.129.115.178.oracle-em1 > 172.128.75.27.ftp: S 541237:541237(0) win 8192 <mss 1460> (DF)
 07:14:05.661634 172.128.75.27.ftp > 192.129.115.178.oracle-em1: S 2928411011:2928411011(0) ack 541238 win 32120 <mss 1460> (DF)
 07:14:05.691809 192.129.115.178.oracle-em1 > 172.128.75.27.ftp: . 1:1(0) ack 1 win 8760 (DF)
 07:14:05.692510 192.129.115.178.oracle-em1 > 172.128.75.27.ftp: F 1:1(0) ack 1 win 8760 (DF)
 07:14:05.692859 192.129.115.178.aspen-services > 172.128.75.27.smtp: S 541286:541286(0) win 8192 <mss 1460> (DF)
 07:14:05.692884 172.128.75.27.ftp > 192.129.115.178.oracle-em1: . 1:1(0) ack 2 win 32120 (DF)
 07:14:05.693101 172.128.75.27.smtp > 192.129.115.178.aspen-services: R 0:0(0) ack 541287 win 0
```

```
 07:14:05.885230 172.128.75.27.gat-lmd > 192.129.115.178.ident: S 2922891838:2922891838(0) win 32120 <mss 1460,sackOK,timestamp 59217772 0,nop,wscale 0>
(DF) 07:14:05.914630 192.129.115.178.ident > 172.128.75.27.gat-lmd: R 0:0(0) ack 2922891839 win 0
 07:14:06.131268 192.129.115.178.aspen-services > 172.128.75.27.smtp: S 541286:541286(0) win 8192 <mss 1460> (DF)
 07:14:06.131555 172.128.75.27.smtp > 192.129.115.178.aspen-services: R 0:0(0) ack 1 win 0
 07:14:06.632144 192.129.115.178.aspen-services > 172.128.75.27.smtp: S 541286:541286(0) win 8192 <mss 1460> (DF)
 07:14:06.632402 172.128.75.27.smtp > 192.129.115.178.aspen-services: R 0:0(0) ack 1 win 0
 07:14:07.133834 192.129.115.178.aspen-services > 172.128.75.27.smtp: S 541286:541286(0) win 8192 <mss 1460> (DF)
 07:14:07.134201 172.128.75.27.smtp > 192.129.115.178.aspen-services: R 0:0(0) ack 1 win 0
 07:14:10.932525 172.128.75.27.ftp > 192.129.115.178.oracle-em1: F 1:1(0) ack 2 win 32120 (DF)
 07:14:10.962454 192.129.115.178.oracle-em1 > 172.128.75.27.ftp: . 2:2(0) ack 2 win 8760 (DF)
 07:14:17.653519 192.129.115.178.iad2 > 172.128.75.27.snmp: GetNextRequest(40) system.sysObjectID system.sysDescr
 07:14:17.653825 172.128.75.27 > 192.129.115.178: icmp: 172.128.75.27 udp port snmp unreachable [tos 0xc0]
 07:14:22.173350 192.129.115.178.iad2 > 172.128.75.27.snmp: GetNextRequest(40) system.sysObjectID system.sysDescr
 07:14:22.173618 172.128.75.27 > 192.129.115.178: icmp: 172.128.75.27 udp port snmp unreachable [tos 0xc0]
 07:14:26.680048 192.129.115.178.iad2 > 172.128.75.27.snmp: GetNextRequest(40) system.sysObjectID system.sysDescr
 07:14:26.680308 172.128.75.27 > 192.129.115.178: icmp: 172.128.75.27 udp port snmp unreachable [tos 0xc0]
                        45c0 006f c1c6 0000 fe01 e31e 8b17 0277
                        95ca f38f 0303 1436 0000 0000 4500 0053
                        761a 0000 7611 b797 95ca f38f 8b17 0277
                        0407 00a1 003f 03fe 3035 0201 0004 0670
                        7562 6c69 63a1 2802 0438 ead6 a902 0100
                        0201 0030 1a30 0b06 072b 0601 0201 0102
                        0500 300b 0607 2b06 0102 0101 0105 00
```

History
- not known

Techniques
- Automated scan: several tries per second
- snmp scan
- Repeated scan

Intent:
- Scan for open ports: ftp, smtp, http

Active targeting
- yes

Result: looks like a scan with the tool snmp-c; dest does not offer these services

---

Detect example #5:

```
 5Apr2000  8:40:45 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 1326
 5Apr2000  8:40:48 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 1326
 5Apr2000  8:40:54 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 1326
 5Apr2000  8:41:06 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 1326
 5Apr2000  8:53:04 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 21 s_port 3216
 5Apr2000  8:53:07 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 21 s_port 3216
 5Apr2000  8:53:13 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 21 s_port 3216
```

```
 5Apr2000  8:53:25 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 21 s_port 3216
 5Apr2000  8:53:49 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 23 s_port 3334
 5Apr2000  8:53:52 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 23 s_port 3334
 5Apr2000  8:53:58 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 23 s_port 3334
 5Apr2000  8:54:10 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 23 s_port 3334
 5Apr2000  8:54:34 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 25 s_port 3417
 5Apr2000  8:54:37 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 25 s_port 3417
 5Apr2000  8:54:43 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 25 s_port 3417
 5Apr2000  8:54:55 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 25 s_port 3417
 5Apr2000  8:55:19 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 79 s_port 3523
 5Apr2000  8:55:22 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 79 s_port 3523
 5Apr2000  8:55:28 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 79 s_port 3523
 5Apr2000  8:55:40 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 79 s_port 3523
 5Apr2000  8:56:04 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 80 s_port 3641
 5Apr2000  8:56:07 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 80 s_port 3641
 5Apr2000  8:56:13 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 80 s_port 3641
 5Apr2000  8:56:25 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 80 s_port 3641
 5Apr2000  8:56:49 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 110 s_port 3773
 5Apr2000  8:56:52 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 110 s_port 3773
 5Apr2000  8:56:58 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 110 s_port 3773
 5Apr2000  8:57:10 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 110 s_port 3773
 5Apr2000  8:57:36 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 3893
 5Apr2000  8:57:39 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 3893
 5Apr2000  8:57:45 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 3893
 5Apr2000  8:57:57 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 139 s_port 3893
 5Apr2000  8:58:21 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 143 s_port 3963
 5Apr2000  8:58:24 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 143 s_port 3963
 5Apr2000  8:58:30 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 143 s_port 3963
 5Apr2000  8:58:43 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 143 s_port 3963
 5Apr2000  8:59:07 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 443 s_port 4027
 5Apr2000  8:59:10 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 443 s_port 4027
 5Apr2000  8:59:16 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 443 s_port 4027
 5Apr2000  8:59:28 drop 172.33.21.19  <hme0 proto tcp src 172.128.75.126 dst 172.46.25.126 service 443 s_port 4027
```

History
- not known

Techniques
- Automated scan, although there is enough time to get responses; source port equal if dest port equal, then changing
- TCP scan
- Repeated scan

Intent:
- Scan for open ports: 21 = ftp, 23 = telnet, 25 = smtp, 79 = finger, 80 = http, 110 = pop3, 139 = nbsession, 143 = imap, 443 = ?

Active targeting
- at least information gathering

Result: Port scan

Detect example #6:

```
 1Feb100  8:04:42 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.1 service 8080 s_port 4614 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.2 service 8080 s_port 4615 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.3 service 8080 s_port 4616 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.4 service 8080 s_port 4617 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.5 service 8080 s_port 4618 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.6 service 8080 s_port 4619 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.7 service 8080 s_port 4620 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.8 service 8080 s_port 4621 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.9 service 8080 s_port 4622 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.10 service 8080 s_port 4623 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.11 service 8080 s_port 4624 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.12 service 8080 s_port 4625 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.13 service 8080 s_port 4626 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.14 service 8080 s_port 4627 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.15 service 8080 s_port 4628 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.16 service 8080 s_port 4629 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.17 service 8080 s_port 4630 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.18 service 8080 s_port 4631 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.19 service 8080 s_port 4632 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.20 service 8080 s_port 4633 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.21 service 8080 s_port 4634 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.22 service 8080 s_port 4635 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.23 service 8080 s_port 4636 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.24 service 8080 s_port 4637 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.25 service 8080 s_port 4638 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.26 service 8080 s_port 4639 rule 180
 1Feb100  8:04:44 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.27 service 8080 s_port 4640 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.28 service 8080 s_port 4641 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.29 service 8080 s_port 4642 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.30 service 8080 s_port 4643 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.31 service 8080 s_port 4644 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.32 service 8080 s_port 4645 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.33 service 8080 s_port 4646 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.34 service 8080 s_port 4647 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.35 service 8080 s_port 4648 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.36 service 8080 s_port 4649 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.37 service 8080 s_port 4650 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.38 service 8080 s_port 4651 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.39 service 8080 s_port 4652 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.40 service 8080 s_port 4653 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.41 service 8080 s_port 4654 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.42 service 8080 s_port 4655 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.43 service 8080 s_port 4656 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.44 service 8080 s_port 4657 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.45 service 8080 s_port 4658 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.46 service 8080 s_port 4659 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.47 service 8080 s_port 4660 rule 180
```

```
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.48 service 8080 s_port 4661 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.49 service 8080 s_port 4662 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.50 service 8080 s_port 4663 rule 180
 1Feb100  8:04:45 drop 172.34.16.78  <hme3 proto tcp src 192.136.218.38 dst 192.128.81.51 service 8080 s_port 4664 rule 180
```

History
- not known

Techniques
- Automated scan: several tries per second, source port increasing continuously
- TCP scan of complete class c net 192.128.81 (The example above is only an excerpt from the complete log)

Intent:
- Scan for open proxies

Active targeting
- yes

Result: Proxy hunter

Detect example #7:

```
 19Jan100 14:14:21 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 53 s_port 2262 rule 180
 19Jan100 14:14:21 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 54 s_port 2263 rule 180
 19Jan100 14:14:21 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 55 s_port 2264 rule 180
 19Jan100 14:14:21 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 56 s_port 2265 rule 180
 19Jan100 14:14:23 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 53 s_port 2262 rule 180
 19Jan100 14:14:23 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 54 s_port 2263 rule 180
 19Jan100 14:14:23 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 55 s_port 2264 rule 180
 19Jan100 14:14:23 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 56 s_port 2265 rule 180
 19Jan100 14:14:29 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 53 s_port 2262 rule 180
 19Jan100 14:14:29 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 54 s_port 2263 rule 180
 19Jan100 14:14:29 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 55 s_port 2264 rule 180
 19Jan100 14:14:29 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 56 s_port 2265 rule 180
 19Jan100 14:14:30 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 57 s_port 2268 rule 180
 19Jan100 14:14:30 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 58 s_port 2269 rule 180
 19Jan100 14:14:30 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 59 s_port 2270 rule 180
 19Jan100 14:14:30 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 60 s_port 2271 rule 180
 19Jan100 14:14:33 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 57 s_port 2268 rule 180
 19Jan100 14:14:33 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 58 s_port 2269 rule 180
 19Jan100 14:14:33 drop 172.33.21.19  <hme3 proto tcp src 192.133.221.190 dst 192.133.221.172 service 59 s_port 2270 rule 180
```

History
- not known

Techniques
- Automated scan: several tries per minute, source and dest port increasing continuously, then are repeated
- TCP scan

```
Intent:
- Scan for open ports


Active targeting
- at least information gathering

Result: Port scan

-------------------------------------------------------------------------------------------------------------------------
Detect example #8:

 15:47:40.132400 172.25.140.16.domain > 172.21.131.87.domain: 0 [0q] Type0 (Class 0)? . (28) (frag 57005:36@0+)
 15:47:40.133353 172.25.140.16 > 172.21.131.87: (frag 57005:4@24)

History
- not known

Techniques
- crafted packets; fragmentation flag is set, but the two fragments overlap (offset in second packet which should be 36 is set to 24)

Intent:
- Denial of service

Active targeting
- yes

Result: teardrop attack

-------------------------------------------------------------------------------------------------------------------------
Detect example #9:

 12:00:01.732490 172.25.140.16.fg-gip > 172.21.131.87.34555: S 3555204546:3555204546(0) win 8192 <mss 1460> (DF)
 12:00:01.732538 172.21.131.87.34555 > 172.25.140.16.fg-gip: R 0:0(0) ack 3555204547 win 0
 12:00:02.186182 172.25.140.16.fg-gip > 172.21.131.87.34555: S 3555204546:3555204546(0) win 8192 <mss 1460> (DF)
 12:00:02.186211 172.21.131.87.34555 > 172.25.140.16.fg-gip: R 0:0(0) ack 1 win 0
 12:00:02.686712 172.25.140.16.fg-gip > 172.21.131.87.34555: S 3555204546:3555204546(0) win 8192 <mss 1460> (DF)
 12:00:02.686737 172.21.131.87.34555 > 172.25.140.16.fg-gip: R 0:0(0) ack 1 win 0
 12:00:03.187334 172.25.140.16.fg-gip > 172.21.131.87.34555: S 3555204546:3555204546(0) win 8192 <mss 1460> (DF)
 12:00:03.187359 172.21.131.87.34555 > 172.25.140.16.fg-gip: R 0:0(0) ack 1 win 0

History
- not known

Techniques
- TCP scan
- Repeated scan

Intent:
```

- Scan for open ports: 34555

Active targeting
- yes

Result: perhaps trin000 master

Detect example #10:

```
 16:05:51.405129 172.25.140.16.rwhois > 172.21.131.87.echo: udp 4294967292
                         4500 0020 dead 0000 fe11 33d4 8b17 ca7d
                         8b17 c99e 10e1 0007 0004 0000 496e 7465
                         7465 7465 7465 7465 7465 7465 7465
```

History
- not known

Techniques
- UDP scan
- Crafted packet: The UDP-lengthfield (25th field counting from 0) contains the value 4. At least a udp-packet must be 8 bytes long, so this is crafted. Tcpdump is not able in this case to compute the length correct, so it computes 4294967292 = 2^32-4.

Intent:
- Denial of service

Active targeting
- yes

Result: udpbomb

Last Updated: July 25th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced