Global Information Assurance Certification Paper

***** Northcutt, good report, Dirk is probably a pro, note the concise analysis where he identifies the detect and moves on the to the next one. 85 *****

Dirk Lehmann, IDIC 2000, 10 Analyzed Detects, Apr 4, 2000

All IP addresses are fictional and do not reflect real addresses.

***** Analyzed Detect #1**

172.33.17.33	23	->	172.81.246.66	23	10-Jan	21:18:14	tcp
172.33.17.33	23	->	172.81.246.50	23	10-Jan	23:19:29	tcp
172.33.17.33	23	->	172.81.246.63	23	10-Jan	23:27:13	tcp
172.33.17.33	23	->	172.81.246.53	23	10-Jan	23:27:17	tcp
172.33.17.33	23	->	172.81.246.48	23	10-Jan	23:45:05	tcp
172.33.17.33	23	->	172.81.246.58	23	11-Jan	4:22:10	tcp
172.33.17.33	23	->	172.81.246.31	23	11-Jan	10:35:21	tcp
172.33.17.33	23	->	172.81.246.19	23	11-Jan	12:42:37	tcp
172.33.17.33	3168	->	172.81.246.54	23	11-Jan	12:42:37	tcp
172.33.17.33	3169	->	172.81.246.54	143	11-Jan	12:42:37	tcp
172.33.17.33	3197	->	172.81.246.51	143	11-Jan	12:42:37	tcp
172.33.17.33	3270	->	172.81.246.19	110	11-Jan	12:42:37	tcp
172.33.17.33	23	->	172.81.246.73	23	11-Jan	12:42:39	tcp
172.33.17.33	23	->	172.81.246.9	23	11-Jan	12:42:45	tcp
172.33.17.33	23	->	172.81.246.68	23	11-Jan	12:42:48	tcp
172.33.17.33	3374	->	172.81.246.68	23	11-Jan	12:42:49	tcp
172.33.17.33	3375	->	172.81.246.68	143	11-Jan	12:42:52	tcp
172.33.17.33	3389	->	172.81.246.49	23	11-Jan	12:42:53	tcp
172.33.17.33	3375	->	172.81.246.68	143	11-Jan	12:42:58	tcp
172.33.17.33	23	->	172.81.246.37	23	11-Jan	12:43:00	tcp
172.33.17.33	143	->	172.81.246.72	143	11-Jan	12:43:08	tcp
172.33.17.33	3375	->	172.81.246.68	143	11-Jan	12:43:09	tcp
172.33.17.33	3391	->	172.81.246.49	110	11-Jan	12:43:12	tcp
172.33.17.33	3460	->	172.81.246.38	2766	11-Jan	12:43:13	tcp
172.33.17.33	3458	->	172.81.246.38	110	11-Jan	12:43:17	tcp
172.33.17.33	3275	->	172.81.246.19	22	11-Jan	12:43:20	tcp
172.33.17.33	3457	->	172.81.246.38	143	11-Jan	12:43:29	tcp
172.33.17.33	3169	->	172.81.246.54	143	11-Jan	12:44:45	tcp
172.33.17.33	3198	->	172.81.246.51	110	11-Jan	12:44:45	tcp
172.33.17.33	3278	->	172.81.246.19	515	11-Jan	12:44:45	tcp
172.33.17.33	3376	->	172.81.246.68	110	11-Jan	12:44:45	tcp
172.33.17.33	3390	->	172.81.246.49	143	11-Jan	12:44:45	tcp
172.33.17.33	3390	->	172.81.246.49	143	11-Jan	12:44:45	tcp
172.33.17.33	3457	->	172.81.246.38	143	11-Jan	12:44:45	tcp
172.33.17.33	3457	->	172.81.246.38	143	11-Jan	12:44:45	tcp
172.33.17.33	3178	->	172.81.246.54	515	11-Jan	12:45:59	tcp
172.33.17.33	3275	->	172.81.246.19	22	11-Jan	12:45:59	tcp
172.33.17.33	3383	->	172.81.246.68	1	11-Jan	12:45:59	tcp
172.33.17.33	3399	->	172.81.246.49	515	11-Jan	12:46:00	tcp
172.33.17.33	3197	->	172.81.246.51	143	11-Jan	12:47:36	tcp
172.33.17.33	3381	->	172.81.246.68	22	11-Jan	12:47:58	tcp
172.33.17.33	3399	->	172.81.246.49	515	11-Jan	12:48:00	tcp
172.33.17.33	3466	->	172.81.246.38	515	11-Jan	12:49:14	tcp
172.33.17.33	3278	->	172.81.246.19	515	11-Jan	12:51:14	tcp
172.33.17.33	3384	->	172.81.246.68	515	11-Jan	12:51:14	tcp
172.33.17.33	3398	->	172.81.246.49	1	11-Jan	12:51:14	tcp
172.33.17.33	3466	->	172.81.246.38	515	11-Jan	12:51:14	tcp
172.33.17.33	3169	->	172.81.246.54	143	11-Jan	12:51:32	tcp
172.33.17.33	3383	->	172.81.246.68	1	11-Jan	12:51:58	tcp
172.33.17.33	3465	->	172.81.246.38	1	11-Jan	12:52:17	tcp
172.33.17.33	3207	->	172.81.246.51	515	11-Jan	12:54:23	tcp
172.33.17.33	3278	->	172.81.246.19	515	11-Jan	12:54:23	tcp
172.33.17.33	3402	->	172.81.246.62	23	11-Jan	12:54:23	tcp
172.33.17.33	3465	->	172.81.246.38	1	11-Jan	12:54:23	tcp

```
172.33.17.33    3178    ->      172.81.246.54   515     11-Jan  12:55:37        tcp
172.33.17.33    2225    ->      172.81.246.54   1       11-Jan  12:55:41        tcp
172.33.17.33    2225    ->      172.81.246.54   1       11-Jan  12:56:47        tcp
172.33.17.33    2228    ->      172.81.246.54   139     11-Jan  12:56:47        tcp
172.33.17.33    2247    ->      172.81.246.19   1       11-Jan  12:56:47        tcp
172.33.17.33    2255    ->      172.81.246.49   12345   11-Jan  12:56:47        tcp
172.33.17.33    3384    ->      172.81.246.68   515     11-Jan  12:56:47        tcp
172.33.17.33    2255    ->      172.81.246.49   12345   11-Jan  12:56:48        tcp
172.33.17.33    2257    ->      172.81.246.68   1       11-Jan  12:56:48        tcp
172.33.17.33    2259    ->      172.81.246.62   1       11-Jan  12:56:48        tcp
172.33.17.33    2259    ->      172.81.246.62   1       11-Jan  12:56:48        tcp
172.33.17.33    2260    ->      172.81.246.68   139     11-Jan  12:56:48        tcp
172.33.17.33    2262    ->      172.81.246.62   139     11-Jan  12:56:48        tcp
172.33.17.33    2262    ->      172.81.246.62   139     11-Jan  12:56:48        tcp
172.33.17.33    2989    ->      172.81.246.30   515     11-Jan  14:03:26        tcp
172.33.17.33    2988    ->      172.81.246.30   1       11-Jan  14:07:26        tcp
172.33.17.33    4242    ->      172.81.246.30   23      11-Jan  14:10:44        tcp
172.33.17.33    4270    ->      172.81.246.30   1       11-Jan  14:10:44        tcp

Analysis:
 Technique:
    + Automated, several connections in one second
    + reuse of source ports, lowest source port 23
    + same target hit at different times
    + not all targets scanned for the same ports
    + TCP scan
    + Host scan and port scan
 Intent:
    + scan for trojan, netbios, imap, ..., what runs on port 1/2766
     telnet             23/tcp
     pop3              110/tcp
     netbios-ssn       139/tcp
     imap              143/tcp
     printer           515/tcp
     NetBus          12345/tcp
 Active Targeting:
    + Yes, but still in information gathering phase.

 Result:
    Looks like the attacker uses some kind of a script that randomizes targets and ports.
System .49 is scanned for Netbus but does not appear somewhere else in the log. Log might
not be complete. Attacker is out for information about systems. Later attacks might
follow.



*** Analyzed Detect #2

9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.1
service 8080 s_port 32073 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.2
service 8080 s_port 32074 rule 186 9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp
src 192.71.102.217 dst 192.138.158.3 service 8080 s_port 32075 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.4
service 8080 s_port 32001 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.5
service 8080 s_port 32002 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.6
service 8080 s_port 32004 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.7
service 8080 s_port 32005 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.8
service 8080 s_port 32006 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst 192.138.158.9
```

```
service 8080 s_port 32007 rule 186
9Mar2000 13:21:56 drop 172.22.23.24  <hme3 proto tcp src 192.71.102.217 dst
192.138.158.10 service 8080 s_port 32008 rule 186

Analysis:
 Technique:
    + Automated, several connections in one second
    + source port increases
    + TCP scan
    + Host scan
 Intent:
    + looking for open proxies
 Active Targeting:
    + Yes, target is 192.138.158.x network

 Result:
    192.71.102.217 tries to find proxies and does not attempt to hide this activity. This
is only an excerpt from the complete log that contains many more connections from the
same system.



*** Analyzed Detect #3


Nov 23 01:45:57 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1251
172.102.45.46:8080 L=44 S=0x00 I=65026 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:00 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1251
172.102.45.46:8080 L=44 S=0x00 I=10755 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:07 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1251
172.102.45.46:8080 L=44 S=0x00 I=22531 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:20 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1251
172.102.45.46:8080 L=44 S=0x00 I=34563 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:46 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1295
172.102.45.46:3128 L=44 S=0x00 I=47107 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:49 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1295
172.102.45.46:3128 L=44 S=0x00 I=58627 F=0x4000 T=6 SYN (#8)
Nov 23 01:46:55 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1295
172.102.45.46:3128 L=44 S=0x00 I=4868 F=0x4000 T=6 SYN (#8)
Nov 23 01:47:08 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:1295
172.102.45.46:3128 L=44 S=0x00 I=19972 F=0x4000 T=6 SYN (#8)
Dec  7 03:00:04 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4433
172.102.45.230:8080 L=44 S=0x00 I=50736 F=0x4000 T=7 SYN (#8)
Dec  7 03:00:07 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4433
172.102.45.230:8080 L=44 S=0x00 I=64304 F=0x4000 T=7 SYN (#8)
Dec  7 03:00:14 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4433
172.102.45.230:8080 L=44 S=0x00 I=10545 F=0x4000 T=7 SYN (#8)
Dec  7 03:00:27 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4433
172.102.45.230:8080 L=44 S=0x00 I=23345 F=0x4000 T=7 SYN (#8)
Dec  7 03:00:53 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4487
172.102.45.230:3128 L=44 S=0x00 I=39729 F=0x4000 T=7 SYN (#8)
Dec  7 03:00:56 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4487
172.102.45.230:3128 L=44 S=0x00 I=51761 F=0x4000 T=7 SYN (#8)
Dec  7 03:01:03 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4487
172.102.45.230:3128 L=44 S=0x00 I=63537 F=0x4000 T=7 SYN (#8)
Dec  7 03:01:16 sneak kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.154.4.145:4487
172.102.45.230:3128 L=44 S=0x00 I=10290 F=0x4000 T=7 SYN (#8)


Analysis:
 Technique:
    + Automated
    + slow, each target and port pair scanned at a different hour
    + several seconds between connections to same target
    + TCP scan
    + always same source port 4487
```

Intent:
+ looking for proxies / Ring Zero
Active Targeting:
+ Yes, probably large network scan but only few systems show up in this log

Result:
Looks like RingZero is running on 172.154.4.145.

***** Analyzed Detect #4**

```
  1Feb100  8:04:39 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.1
service 8080 s_port 4614 rule 180
  1Feb100  8:04:42 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.1
service 8080 s_port 4614 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.2
service 8080 s_port 4615 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.3
service 8080 s_port 4616 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.4
service 8080 s_port 4617 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.5
service 8080 s_port 4618 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.6
service 8080 s_port 4619 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.7
service 8080 s_port 4620 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.8
service 8080 s_port 4621 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.9
service 8080 s_port 4622 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.10
service 8080 s_port 4623 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.11
service 8080 s_port 4624 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.12
service 8080 s_port 4625 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.13
service 8080 s_port 4626 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.14
service 8080 s_port 4627 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.15
service 8080 s_port 4628 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.16
service 8080 s_port 4629 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.17
service 8080 s_port 4630 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.18
service 8080 s_port 4631 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.19
service 8080 s_port 4632 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.20
service 8080 s_port 4633 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.21
service 8080 s_port 4634 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.22
service 8080 s_port 4635 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.23
service 8080 s_port 4636 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.24
service 8080 s_port 4637 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.25
service 8080 s_port 4638 rule 180
```

```
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.26
service 8080 s_port 4639 rule 180
  1Feb100  8:04:44 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.27
service 8080 s_port 4640 rule 180
  1Feb100  8:04:45 drop 172.22.23.24  <hme3 proto tcp src 192.231.86.124 dst 172.1.81.28
service 8080 s_port 4641 rule 180

Analysis:
 Technique:
    + Automated, several connections in one second
    + source port increases by one
    + TCP scan
    + Host scan
 Intent:
    + looking for proxies
 Active Targeting:
    + Yes, 172.1.81.x network

 Result:
    Again someone looking for proxies. 24 connection attempts in one second will clearly
stand up in the log file. 192.231.86.124 does not attempt to hide its activity.



*** Analyzed Detect #5

 20Aug99 23:18:02 drop 1.2.3.4  <nf0 proto udp src 172.24.25.5 dst 172.20.3.113 service
domain-udp s_port 3379 rule 156
 20Aug99 23:18:09 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
echo-tcp s_port 3531 rule 156
 20Aug99 23:18:15 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
echo-tcp s_port 3531 rule 156
 20Aug99 23:18:16 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
ftp s_port 3626 rule 156
 20Aug99 23:18:22 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
ftp s_port 3626 rule 156
 20Aug99 23:18:22 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
gopher s_port 3722 rule 156
 20Aug99 23:18:27 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
nntp s_port 3817 rule 156
 20Aug99 23:18:27 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
pop-3 s_port 3912 rule 156
 20Aug99 23:18:30 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
pop-3 s_port 3912 rule 156
 20Aug99 23:18:31 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
smtp s_port 4007 rule 156
 20Aug99 23:18:36 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
time-tcp s_port 4102 rule 156
 20Aug99 23:18:36 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
SecureWeb-ZF s_port 4197 rule 156
 20Aug99 23:18:40 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
SecureWeb-ZF s_port 4197 rule 156
 20Aug99 23:18:40 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
IMAP4 s_port 4292 rule 156
 20Aug99 23:18:42 drop 1.2.3.4  <nf0 proto tcp src 172.24.25.5 dst 172.20.3.113 service
IMAP4 s_port 4292 rule 156

Analysis:
 Technique:
    + Probably automated: many ports, some connections in one second
    + a gap in time is refelected by a jump of the source port -> system does other
networking as well
    + TCP scan
    + Port scan
 Intent:
    + looking for vulnerable services / fingerprinting
```

Active Targeting:
+ Yes

Result:
172.24.25.5 tries to gather information about target for probably later attacks.

***** Analyzed Detect #6**

DATE	TIME	SIP	SPORT	DIP	DPORT	SIG_NAME
2000-01-10	21:18:15	172.33.17.33	3506	172.81.246.12	53	DNS High Zone Xfer
2000-01-10	22:44:34	172.33.17.33	4720	172.81.246.12	53	DNS High Zone Xfer
2000-01-10	22:52:50	172.33.17.33	3593	172.81.246.11	53	DNS High Zone Xfer
2000-01-10	23:45:03	172.33.17.33	1982	172.81.246.12	53	DNS High Zone Xfer
2000-01-11	02:00:22	172.33.17.33	4757	172.81.246.12	53	DNS High Zone Xfer
2000-01-11	02:00:24	172.33.17.33	4777	172.81.246.56	111	TCP Port Sweep
2000-01-11	02:00:24	172.33.17.33	4781	172.81.246.56	22	TCP SYN Port Sweep
2000-01-11	02:00:25	172.33.17.33	5	172.81.246.56	80	TCP Packet, No Flags
2000-01-11	02:00:25	172.33.17.33	4	172.81.246.56	80	TCP Packet, SYN & FIN Only
2000-01-11	02:00:25	172.33.17.33	2	172.81.246.56	80	TCP Packet, FIN Only
2000-01-11	02:00:25	172.33.17.33	5	172.81.246.56	80	Queso Sweep
2000-01-11	04:22:09	172.33.17.33	3508	172.81.246.12	53	DNS High Zone Xfer
2000-01-11	10:34:36	172.33.17.33	2225	172.81.246.11	53	DNS High Zone Xfer
2000-01-11	11:23:22	172.33.17.33	1747	172.81.246.11	53	DNS High Zone Xfer
2000-01-11	11:31:45	172.33.17.33	3205	172.81.246.12	53	DNS High Zone Xfer
2000-01-11	12:42:22	172.33.17.33	3135	172.81.246.12	53	DNS High Zone Xfer
2000-01-11	12:42:31	172.33.17.33	3183	172.81.246.16	80	TCP Port Sweep
2000-01-11	12:42:31	172.33.17.33	3189	172.81.246.16	25	TCP SYN Port Sweep
2000-01-11	12:42:35	172.33.17.33	3237	172.81.246.21	1	TCP Port Sweep
2000-01-11	12:42:35	172.33.17.33	3238	172.81.246.21	515	TCP SYN Port Sweep
2000-01-11	12:42:35	172.33.17.33	5	172.81.246.16	25	TCP Packet, No Flags
2000-01-11	12:42:35	172.33.17.33	4	172.81.246.16	25	TCP Packet, SYN & FIN Only
2000-01-11	12:42:41	172.33.17.33	2	172.81.246.21	23	TCP Packet, FIN Only
2000-01-11	12:42:41	172.33.17.33	5	172.81.246.21	23	Queso Sweep
2000-01-11	12:56:02	172.33.17.33	5	172.81.246.49	80	Queso Sweep
2000-01-11	12:56:03	172.33.17.33	5	172.81.246.62	80	Queso Sweep
2000-01-11	13:06:33	172.33.17.33	3537	172.81.246.12	53	DNS High Zone Xfer

Analysis:

Technique:
- + Automated, several scans in one second
- + large gaps in time, scan over two days
- + TCP scan
- + Port scan
- + crafted packets

Intent:
- + fingerprinting, zone transfer attempts, scanning through firewall

Active Targeting:
- + Yes, information gathering and zone xfers

Result:

172.33.17.33 scans several systems on the network using stealth techniques. Probably the attacker has three tools running on his system. QueSO, another one for the stealth scans, and one for zone transfers. Or he just uses NMAP. Anyway, this is information gathering. Attacker is root on his system because he can craft packets. But why does he use a high port for DNS Zone transfers?

***** Analyzed Detect #7**

172.8.6.203	2328 ->	172.81.246.0	80	Jan 22	08:59:54	tcp
172.8.6.203	2329 ->	172.81.246.3	80	Jan 22	08:59:55	tcp
172.8.6.203	2641 ->	172.81.246.75	80	Jan 22	08:59:56	tcp
172.8.6.203	2642 ->	172.81.246.75	80	Jan 22	08:59:57	tcp
172.8.6.203	2326 ->	172.81.246.144	80	Jan 22	08:59:58	tcp
172.8.6.203	2327 ->	172.81.246.144	80	Jan 22	08:59:59	tcp
172.8.6.203	1610 ->	172.81.246.200	80	Jan 22	09:00:00	tcp
172.8.6.203	1372 ->	172.81.246.231	80	Jan 22	09:00:01	tcp

Analysis:

Technique:
- + Automated, every second one connection
- + source port varies, there seem to be pairs of source ports
- + TCP scan

Intent:
- + looking for web servers

Active Targeting:
- + Yes, target might be 172.81.246.x network or targeted IPs randomly chosen.

Result:

172.8.6.203 searches for web servers. .0 is usually the broadcast address. So why does he try to make a TCP connection to this IP? Maybe he just don't know?

***** Analyzed Detect #8**

172.204.135.157	110 ->	172.81.246.11	110	27-May	3:37:14	tcp
172.204.135.157	29396 ->	172.81.246.11	23	27-May	3:37:44	tcp
172.204.135.157	29812 ->	172.81.246.12	110	27-May	3:37:44	tcp
172.204.135.157	29390 ->	172.81.246.11	80	27-May	3:37:47	tcp
172.204.135.157	29757 ->	172.81.246.12	23	27-May	3:37:48	tcp
172.204.135.157	29443 ->	172.81.246.11	110	27-May	3:37:53	tcp
172.204.135.157	29813 ->	172.81.246.12	111	27-May	3:37:54	tcp
172.204.135.157	29812 ->	172.81.246.12	110	27-May	3:38:14	tcp
172.204.135.157	29444 ->	172.81.246.11	111	27-May	3:38:42	tcp
172.204.135.157	29813 ->	172.81.246.12	111	27-May	3:38:58	tcp
172.204.135.157	17293 ->	172.81.246.11	23	27-May	3:40:53	tcp
172.204.135.157	29446 ->	172.81.246.11	79	27-May	3:40:56	tcp
172.204.135.157	2 ->	172.81.246.12	23	27-May	3:40:57	tcp
172.204.135.157	29913 ->	172.81.246.12	21	27-May	3:41:02	tcp
172.204.135.157	29982 ->	172.81.246.12	22	27-May	3:41:03	tcp
172.204.135.157	20331 ->	172.81.246.11	143	27-May	3:41:05	tcp

```
172.204.135.157 20559   ->      172.81.246.12   80      27-May  3:41:07 tcp
172.204.135.157 20924   ->      172.81.246.11   80      27-May  3:41:09 tcp
172.204.135.157 17293   ->      172.81.246.11   23      27-May  3:44:33 tcp
172.204.135.157 19400   ->      172.81.246.12   23      27-May  3:45:57 tcp
172.204.135.157 19922   ->      172.81.246.11   139     27-May  3:46:57 tcp


Analysis:
 Technique:
    + Automated, two connections in one second
    + reuse of source port numbers, low source port of 2, source port numbers decrease
and increase -> crafted?
    + TCP scan
    + Port scan
 Intent:
    + looking for information and vulnerable services
      ftp                21/tcp
      telnet             23/tcp
      finger             79/tcp
      http               80/tcp
      pop3              110/tcp
      sunrpc            111/tcp
      sunrpc            111/udp
      netbios-ssn       139/tcp
      imap              143/tcp
 Active Targeting:
    + Yes, targets are 172.81.246.12 and .11

 Result:
    172.204.135.157 tries to gather information about the target systems. Maybe he wants
to attack later. Source ports 2 and 110 do not fit into the picture. No idea what that
means.



*** Analyzed Detect #9


Oct 18 08:40:26 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=47440 F=0x0000 T=109 (#5)
Oct 18 08:40:35 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=45622 F=0x0000 T=109 (#5)
Oct 18 08:40:40 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=49358 F=0x0000 T=109 (#5)
Oct 18 08:40:51 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=18633 F=0x0000 T=109 (#5)
Oct 18 08:40:53 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=62741 F=0x0000 T=109 (#5)
Oct 18 08:40:54 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=65323 F=0x0000 T=109 (#5)
Oct 18 08:41:41 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.116:1234 L=40 S=0x00 I=22475 F=0x0000 T=109 (#5)
Oct 18 09:41:46 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=27044 F=0x0000 T=109 (#5)
Oct 18 09:41:58 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=17108 F=0x0000 T=109 (#5)
Oct 18 09:42:21 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=10277 F=0x0000 T=109 (#5)
Oct 18 09:42:21 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=20775 F=0x0000 T=109 (#5)
Oct 18 09:42:25 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=12913 F=0x0000 T=109 (#5)
Oct 18 09:43:25 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.127:1089 L=40 S=0x00 I=56182 F=0x0000 T=109 (#5)
Oct 18 16:40:28 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
```

```
172.102.45.35:1234 L=40 S=0x00 I=21075 F=0x0000 T=109 (#6)
Oct 18 16:41:13 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.35:1234 L=40 S=0x00 I=62089 F=0x0000 T=109 (#6)
Oct 18 16:41:22 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.35:1234 L=40 S=0x00 I=42552 F=0x0000 T=109 (#6)
Oct 18 16:41:27 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.35:1234 L=40 S=0x00 I=52366 F=0x0000 T=109 (#6)
Oct 18 16:42:12 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.35:1234 L=40 S=0x00 I=25823 F=0x0000 T=109 (#6)
Oct 18 16:44:30 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.35:1234 L=40 S=0x00 I=60899 F=0x0000 T=109 (#6)
Oct 18 17:42:37 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.46:1089 L=40 S=0x00 I=1433 F=0x0000 T=110 (#6)
Oct 18 17:42:50 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.46:1089 L=40 S=0x00 I=36745 F=0x0000 T=110 (#6)
Oct 18 17:43:42 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.46:1089 L=40 S=0x00 I=5454 F=0x0000 T=110 (#6)
Oct 18 17:43:58 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.46:1089 L=40 S=0x00 I=65406 F=0x0000 T=110 (#6)
Oct 18 17:44:04 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6 172.173.124.126:21
172.102.45.46:1089 L=40 S=0x00 I=15085 F=0x0000 T=110 (#6)

Analysis:
 Technique:
    + Automated
    + slow, each target and port pair scanned at a different hour
    + several seconds between connections to same target
    + UDP scan
    + always same source port 21 (FTP)
 Intent:
    + looking for trojans (1234 = Ultors Trojan, 1089 = ?)
 Active Targeting:
    + Yes, but the attacker does not seem to know whether the trojan runs on the target
system.

 Result:
    Probably large network scan but only few systems show up in this log. Target systems
could as well be randomly chosen. Seems like that the source system rotates through the
two target ports. Attacker uses source port 21 to hide in FTP traffic.
    Which trojan is on 1089?



*** Analyzed Detect #10


Oct 19 10:33:04 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1121 172.98.144.2:23 L=44 S=0x10 I=6225 F=0x4000 T=51 SYN (#6)
Oct 19 10:33:07 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1121 172.98.144.2:23 L=44 S=0x10 I=6367 F=0x4000 T=51 SYN (#6)
Oct 19 10:33:13 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1121 172.98.144.2:23 L=44 S=0x10 I=6814 F=0x4000 T=51 SYN (#6)
Oct 19 10:33:25 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1121 172.98.144.2:23 L=44 S=0x10 I=7376 F=0x4000 T=51 SYN (#6)
Oct 19 10:33:49 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1121 172.98.144.2:23 L=44 S=0x10 I=7629 F=0x4000 T=51 SYN (#6)
Oct 19 10:43:13 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1880 172.98.144.2:23 L=44 S=0x10 I=30372 F=0x4000 T=51 SYN (#6)
Oct 19 10:43:15 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1880 172.98.144.2:23 L=44 S=0x10 I=30379 F=0x4000 T=51 SYN (#6)
Oct 19 10:43:21 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1880 172.98.144.2:23 L=44 S=0x10 I=30387 F=0x4000 T=51 SYN (#6)
Oct 19 10:43:33 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1880 172.98.144.2:23 L=44 S=0x10 I=30442 F=0x4000 T=51 SYN (#6)
Oct 19 10:43:57 cobra kernel: Packet log: bad-dmz DENY eth1 PROTO=6
172.221.87.10:1880 172.98.144.2:23 L=44 S=0x10 I=30863 F=0x4000 T=51 SYN (#6)
```

Analysis:
Technique:
+ Automated, connection attempts in intervals of 3/6/12/24 seconds
+ reuse of source port numbers
+ TCP "scan"
Intent:
+ looking for telnet
Active Targeting:
+ Yes

Result:
Probably a user who tried to connect to telnet. Since no answer came back the system retried the connection attempt after a predefined timeout period.

Last Updated: July 24th, 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 Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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
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
SANS Baltimore Fall 2017	Baltimore, MD	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
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 Seattle 2017	Seattle, WA	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