Global Information Assurance Certification Paper

*** Northcutt, kinda tough when the detects aren't numbered, but assuming networkice knows a PCanywhere ping then it is UDP and that leaves SSH out. 74 *

Intrusion Detection Analysis Exam Practical

By: Lisa Ann Kiekow

My name is Lisa Kiekow and I am a Security Technical Analyst. My daily duties include responding to abuse mail, interpreting firewall logs, investigating complaints from our customers regarding intrusion attempts, and processing subpoenas and other legal documents relating to Internet Abuse. I attended the SANS 2000 conference to gain a better understanding of how to interpret both our internal and our customers' firewall logs. I decided that the Immersion Detection Curriculum was best for my needs.

After I completed the courses offered in the IDIC, I took a test that is part of the process to become certified. The other part of this certification was the practical part. Upon passing the test offered during SANS 2000 Intrusion Detection Immersion Curriculum, I researched ten different firewall logs. Many of them are very interesting, and have proved to be a very good learning experience for me. After attending the SANS conference, I never looked at the logs I investigate every day, the same.

The following files are the firewall logs that I did an analysis of in order. They are actually ten separate files condensed into one. Enjoy!

---

1. Identify hostile individuals and groups: A web hosting firm.

   2. Identify their history: No previous history found.

   3. Identify their techniques: They are targeting DNS servers that are open to zone transfers.

   4. Evidence of intent: To find information via a zone transfer on the target DNS servers.

   5. Evidence of active targeting: Yes!

   6. Evaluation of information: Logs from bind below clearly show blocked zone transfer attempts. After contacting the party responsible, they denied they were attempting zone transfers, but that they were simply doing "web surveying". Clearly that is not the case. I rate this incident on the Infocon System scale as a yellow, which is the initial level of heightened alert. I rated this yellow because the party responsible was unsuccessful, however this traffic is suspicious and should be kept under a watchful eye.

Begin Logs:

> > Mar 26 23:50:03 gatekeeper syslogs: Log: MANSYSDAILY: Log files for
> > 26032000 archived.
> > Mar 26 23:56:27 gatekeeper dnsxd: Warning: READFAIL: read system call
> > failed: Interrupted system call
> > Mar 26 23:57:01 gatekeeper dnsxd: Warning: READFAIL: read system call
> > failed: Interrupted system call
> > Mar 26 23:57:25 gatekeeper dnsxd: Warning: READFAIL: read system call
> > failed: Interrupted system call
> > Mar 27 00:12:13 gatekeeper dnsxd: Warning: BADZTREQ: remote host
> > [xxx.xxx.xxx.xx]/xxx.xxx.xxx.xxx attempted to perform a zone transfer
> > Mar 27 00:12:13 gatekeeper dnsxd: Event: EVENTMSG: event badredzt
> > detected from host [xxx.xxx.xxx.xxx]/xxx.xxx.xxx.xxx> > Mar 27 00:12:13
gatekeeper dfw: Log: GOTEVENT: event 'dnsxd.badredzt'
> > from xxx.xxx.xxx.xxx detected by alarm daemon
> > Mar 27 00:12:13 gatekeeper dfw: Alarm: ALARMMSG: alarm daemon
generating
> > an alarm in state YELLOW
> > Mar 27 00:12:13 gatekeeper dnsxd: Warning: READFAIL: read system call
> > failed: Interrupted system call
> > Mar 27 00:14:21 gatekeeper dnsxd: Warning: BADZTREQ: remote host
> > [xxx.xxx.xxx.xxx]/xxx.xxx.xxx.xxx attempted to perform a zone transfer
> > Mar 27 00:14:21 gatekeeper dnsxd: Event: EVENTMSG: event badredzt
> > detected from host [xxx.xxx.xxx.xxx]/xxx.xxx.xxx.xxx> > Mar 27 00:14:22
gatekeeper dfw: Log: GOTEVENT: event 'dnsxd.badredzt'
> > from xxx.xxx.xxx.xxx detected by alarm daemon
> > Mar 27 00:14:22 gatekeeper dfw: Alarm: ALARMMSG: alarm daemon
generating
> > an alarm in state YELLOW
> > Mar 27 00:15:18 gatekeeper dnsxd: Warning: BADZTREQ: remote host
> > []xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx attempted to perform a zone transfer
> > Mar 27 00:15:18 gatekeeper dnsxd: Event: EVENTMSG: event badredzt
> > detected from host [xxx.xxx.xxx.xxx]/>xxx.xxx.xxx.xxx > Mar 27 00:15:18
gatekeeper dfw: Log: GOTEVENT: event 'dnsxd.badredzt'
> > from xxx.xxx.xxx.xxx detected by alarm daemon
> > Mar 27 00:15:18 gatekeeper dfw: Alarm: ALARMMSG: alarm daemon
generating
> > an alarm in state YELLOW
> > Mar 27 00:16:48 gatekeeper dnsxd: Warning: BADZTREQ: remote host
> > [xxx.xxx.xxx.xxx]/xxx.xxx.xxx.xxx attempted to perform a zone transfer
> > Mar 27 00:16:48 gatekeeper dnsxd: Event: EVENTMSG: event badredzt
> > detected from host [xxx.xxx.xxx.xxx]/xxx.xxx.xxx.xxx> > Mar 27 00:16:49
gatekeeper dfw: Log: GOTEVENT: event 'dnsxd.badredzt'
> > from xxx.xxx.xxx.xxx detected by alarm daemon
> > Mar 27 00:16:49 gatekeeper dfw: Alarm: ALARMMSG: alarm daemon

generating
> > an alarm in state YELLOW

End Logs

Identify Hostile Individuals and Groups: A dialup account

Identify their History: No known history

Identify their Techniques: A fast, automated vulnerability scan on Telnet and SunRPC ports spanning 2 days and generally lasting a few seconds.

Evidence of Intent? The attacker's intent is possibly reconisance by scanning for telnet and scanning for vulnerabilities.

Evidence of Active Targeting: There is no evidence of active targeting being whereas this scan spanned a large number of addresses.

Evaluation of Information: This attacker is attempting to gain information by scanning the Telnet port and is also searching for vulnerabilities on many different hosts on the same network. The attacker is targeting two ports known for their vulnerabilities, namely Telnet and Sun RPC. I rate this intrusion attempt a Yellow due to the fact that the attacker was not successful and was detected, however heightened awareness and a watchful eye should be kept on the logs to observe any more attempts from this attacker.

Logs Begin:

- Source Destination

> list 100 denied tcp xxx.xxx.xxx.xxx(3762) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:37 victim.com .com 367: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3833) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:41 victim.com 368: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3926) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:42 victim.com 369: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3790) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:44 victim.com 370: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3926) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:45 victim.com 371: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3832) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:45 victim.com 372: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3833) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:47 victim.com 373: 3d12h: %SEC-6-IPACCESSLOGP:

> list 100 denied tcp xxx.xxx.xxx.xxx(3834) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:47 victim.com 374: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3921) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 2 07:46:50 victim.com 375: 3d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3926) -> xxx.xxx.xxx.xxx(23), 1 packet
> Apr 3 05:00:54 victim.com 451: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4605) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:00:55 victim.com 452: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4645) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:00:59 victim.com 453: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4707) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:00 victim.com 454: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4608) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:01 victim.com 455: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4643) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:02 victim.com 456: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4737) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:05 victim.com 457: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4707) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:06 victim.com 458: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4715) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:07 victim.com 459: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4734) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 05:01:08 victim.com 460: 4d09h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(4737) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 07:53:36 victim.com 462: 4d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3149) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 07:53:39 victim.com 463: 4d12h: %SEC-6-IPACCESSLOGP:
> list 100 denied tcp xxx.xxx.xxx.xxx(3148) -> xxx.xxx.xxx.xxx(111), 1 packet
> Apr 3 07:53:40 victim.com 464: 4d12h: %SEC-6-IPACCESSLOGP:

➢

Logs End

Identify Hostile Individuals and Groups: A dial up account.

Identify their History: No history available.

Identify their Techniques: The attacker is using an automated script to find backdoors, or vulnerabilities by doing a fast port scan for Portmapper/SunRPC and port 10752 which is the port that one of the many Linux mountd (port 635) exploits installs its backdoor at. The bx.c IRC exploit puts a root shell also can place a backdoor listening at this port.

Evidence of Intent? The intention of this attacker appears to be to find a backdoor into 2 DNS servers on the same network.

Evidence of Active Targeting: Yes, the attackers are actively targeting 2 specific DNS servers and are targeting ports 111 and 10752.

Evaluation of Information: The attacker is trying to gain entry through two ports with well-known vulnerabilities into two DNS servers located on the same network. The attacker may also be attempting to gain knowledge of the port on these DNS servers through port 111. The Infocon System rating I am choosing for this incident is yellow. The attacker was not successful however this should be monitored.

Logs Begin:

Source Destination

Apr 3 16:54:05 src=xxx.xxx.xxx.xxx dst= xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:05 src= xxx.xxx.xxx.xxx dst= xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:09 src= xxx.xxx.xxx.xxx dst= xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:09 src= xxx.xxx.xxx.xxx dst= xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:15 src= xxx.xxx.xxx.xxx dst= xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:15 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:19 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:19 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:23 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:23 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:29 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:29 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:33 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:33 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:39 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:39 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:43 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:43 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:49 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:49 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:53 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:53 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:54:59 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=901 dst_port=111
Apr 3 16:54:59 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=906 dst_port=111
Apr 3 16:55:09 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:55:09 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:55:11 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:55:12 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:55:18 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:55:18 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:55:30 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:55:30 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:55:54 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:55:54 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:56:42 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:56:42 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 16:58:17 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 16:58:17 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 17:02:18 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752

Apr 3 17:02:18 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752
Apr 3 17:04:17 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3703 dst_port=10752
Apr 3 17:04:17 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx src_port=3705 dst_port=10752

Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: No history available.

Identify their Techniques: An automated port scan on UDP port 137, which is the Netbios name service, on many different hosts on this network.

Evidence of Intent? To scan for an open port 137 to gain entry to the hosts systems vulnerable, or determine whether the host is running a Windows OS or running Samba on a Unix system.

Evidence of Active Targeting: No, due to the large amount of addresses scanned.

Evaluation of Information: This is an fast automated scan of a subnet for UDP port 137 which if left open and vulnerable can gain the attacker access to the victim's drive. This scan can also tell the attacker whether or not these hosts are running a Windows Operating system or running Samba so that the attacker knows which vulnerabilities to take advantage of and what exploits to run. The Infocon system level is yellow for the need for heightened awareness but is not orange due to the fact this scan was stopped at the Firewall which appears to be working properly.

Logs Begin:

Source Destination

Apr 3 14:27:46 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.1.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:28:03 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.2.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:28:13 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.3.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:28:25 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.4.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:28:42 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.5.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:28:57 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.6.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:29:10 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.7.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:29:22 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.8.137

(3 times, 0/0 src/dest port variations)
Apr 3 14:29:36 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.9.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:29:52 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.10.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:30:10 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.11.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:30:21 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.12.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:30:31 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.13.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:30:46 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.14.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:31:00 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.15.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:31:15 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.16.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:31:27 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.17.137
(2 times, 0/0 src/dest port variations)
Apr 3 14:31:37 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.18.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:31:51 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.19.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:32:07 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.20.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:32:22 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.21.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:32:36 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.22.137
(2 times, 0/0 src/dest port variations)
Apr 3 14:32:52 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.23.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:33:03 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.24.137
(3 times, 0/0 src/dest port variations)
Apr 3 14:33:17 deny: UDP from xxx.xxx.xxx.xxx.137 to xxx.xxx.xxx.25.137
Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: Intrusion attempt has spanned 2 days.

Identify their Techniques: A slow deliberated scan on port 22 for PCAnywhere or the SSH vulnerability.

Evidence of Intent? To scan for an open port 22 and if open use PCAnywhere or SSH to remotely gain access and control of the vulnerable host.

Evidence of Active Targeting: No, there is not enough information to determine this.

Evaluation of Information: This intrusion attempt is a slow focused scan, spanning 2 days, on one specific host for an open port 22. If this port were accessible the attacker would then gain entry and control of the victim host. The Infocon system rating I would give this intrusion attempt is yellow for heightened alert.

Logs Begin:

#File format help at: http://www.networkice.com/Advice/Support/KB/q000018/
#Severity, timestamp (GMT), issueId, issueName, intruderIp, intruderName, victimIp, victimName, parameters, count
19, 2000-04-05 23:38:45, 2001507, PCAnywhere ping, xxx.xxx.xxx.xxx, intrudername, xxx.xxx.xxx.xxx, port=22, 5
19, 2000-04-06 01:24:21, 2001507, PCAnywhere ping, xxx.xxx.xxx.xxx, intrudername, xxx.xxx.xxx.xxx, port=22, 1
19, 2000-04-06 17:31:17, 2001507, PCAnywhere ping, xxx.xxx.xxx.xxx, intrudername, xxx.xxx.xxx.xxx, port=22, 4

Logs End

Identify Hostile Individuals and Groups: A dialup account.

Identify their History: Attacker has a history of attempts on the victim's machine after an argument with victim on IRC chat.

Identify their Techniques: This is a fast, automated scan about every four seconds for trojans and every other vulnerability under the sun.

Evidence of Intent? Yes, blatantly malicious intentions displayed towards victim.

Evidence of Active Targeting: Yes, the victim has been targeted by the attacker before; these logs show the attacker targets only the victim's machine and not an address range.

Evaluation of Information: This is a very fast, automated port scan targeting the victim host machine for every vulnerability imaginable. Just a few of the many targeted port include: Netbus (12346), Netbus 2 Pro (20034), Back Oriface (31337), Subseven trojan (1243),Deap Throat (6670) , Millenium (2000), Devil (65000) and Netmonitor (7306). I rate this a yellow on the Infocon System for heightened alert. The attacker did not

successfully get past the victim's firewall, but appears determined by the numbers of attempts, ports scanned, and the fact that the attacker has tried this before.

Logs Begin:

date & time of attack : attacker IP address Host IP #

```
---------------------------- -------------------------- ------------
FWIN,2000/04/06,19:37:00 -8:00 GMT,victim:1156,attacker:12346,TCP
FWIN,2000/04/06,19:37:08 -8:00 GMT,victim:1157,attacker:20034,TCP
FWIN,2000/04/06,19:37:12 -8:00 GMT,victim:1158,attacker:31337,TCP
FWIN,2000/04/06,19:37:16 -8:00 GMT,victim:1159,attacker:1243,TCP
FWIN,2000/04/06,19:37:20 -8:00 GMT,victim:1160,attacker:30100,TCP
FWIN,2000/04/06,19:37:24 -8:00 GMT,victim:1161,attacker:6670,TCP
FWIN,2000/04/06,19:37:32 -8:00 GMT,victim:1162,attacker:31,TCP
FWIN,2000/04/06,19:37:36 -8:00 GMT,victim:1163,attacker:1001,TCP
FWIN,2000/04/06,19:37:44 -8:00 GMT,victim:1164,attacker:20000,TCP
FWIN,2000/04/06,19:37:48 -8:00 GMT,victim:1165,attacker:65000,TCP
FWIN,2000/04/06,19:37:52 -8:00 GMT,victim:1166,attacker:7306,TCP
FWIN,2000/04/06,19:37:56 -8:00 GMT,victim:1167,attacker:1170,TCP
FWIN,2000/04/06,19:38:00 -8:00 GMT,victim:1168,attacker:5000,TCP
FWIN,2000/04/06,19:38:04 -8:00 GMT,victim:1169,attacker:30303,TCP
FWIN,2000/04/06,19:38:08 -8:00 GMT,victim:1170,attacker:6969,TCP
FWIN,2000/04/06,19:38:12 -8:00 GMT,victim:1171,attacker:61466,TCP
FWIN,2000/04/06,19:38:16 -8:00 GMT,victim:1172,attacker:12076,TCP
FWIN,2000/04/06,19:38:20 -8:00 GMT,victim:1173,attacker:4950,TCP
FWIN,2000/04/06,19:38:24 -8:00 GMT,victim:1174,attacker:16969,TCP
FWIN,2000/04/06,19:38:28 -8:00 GMT,victim:1175,attacker:1245,TCP
FWIN,2000/04/06,19:41:54 -8:00 GMT,victim:1226,attacker:10607,TCP
FWIN,2000/04/06,19:41:58 -8:00 GMT,victim:1227,attacker:3587,TCP
FWIN,2000/04/06,19:42:04 -8:00 GMT,victim:1228,attacker:1042,TCP
FWIN,2000/04/06,19:42:06 -8:00 GMT,victim:1229,attacker:2283,TCP
FWIN,2000/04/06,19:42:10 -8:00 GMT,victim:1230,attacker:5400,TCP
FWIN,2000/04/06,19:42:14 -8:00 GMT,victim:1231,attacker:1010,TCP
FWIN,2000/04/06,19:42:18 -8:00 GMT,victim:1232,attacker:1015,TCP
```

Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: Logs of this intrusion attempt are from a CERT in France.

Identify their Techniques: Very fast, targeted, automated scan for port 27374.

Evidence of Intent? The intent appears to be to scan many hosts on the victim's subnet for port 27374 the Subseven Version 2 trojan port to gain entry.

Evidence of Active Targeting: No, because it is a scan of a number of addresses.

Evaluation of Information: This was an unsuccessful intrusion attempt to gain entry into the scanned hosts through the Subseven Version 2 port 27374. This is a targeted port scan for a specific vulnerability. The Infocon System rating I give this attempt is a yellow for heightened alert.

Logs Begin:

> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/1997 dst > dmz:xxx.xxx.100.1/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/1999 dst > dmz:xxx.xxx.100.3/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2000 dst > dmz:xxx.xxx.100.4/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2001 dst > dmz:xxx.xxx.100.5/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/1998 dst > dmz:xxx.xxx.100.2/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2002 dst > dmz:xxx.xxx.100.6/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2003 dst > dmz:xxx.xxx.100.7/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2004 dst > dmz:xxx.xxx.100.8/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2005 dst > dmz:xxx.xxx.100.9/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2006 dst > dmz:xxx.xxx.100.10/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2007 dst > dmz:xxx.xxx.100.11/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2008 dst > dmz:xxx.xxx.100.12/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2009 dst > dmz:xxx.xxx.100.13/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2010 dst > dmz:xxx.xxx.100.14/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2011 dst > dmz:xxx.xxx.100.15/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2012 dst > dmz:xxx.xxx.100.16/27374
> Apr 9 19:52:30 victim.xxx Apr 09 2000 19:52:25: %PIX-3-106010: Deny inbound tcp src outside:intruder/2013 dst outside:209.180.159.

Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: No history available.

Identify their Techniques: A port scan for port 161.

Evidence of Intent? To gain information, entry, or control of the victim's host machines through an open SNMP port.

Evidence of Active Targeting: No, because there is no proof as to whether or not these machines were scanned specifically or as part of a larger scan of a class B or C.

Evaluation of Information: This intrusion attempt is a scan over the victim's hosts for the SNMP port 161. When looking at the actual dump of the packet, one can see that the intruder is checking to see if the defaults are set to allow public read-only access which would give the intruder much information about the network. If this were the case, the attacker would probably come back and check for the private default, and if that was the configuration, gain entry. The Infocon system rating is yellow for heightened alert, due to the fact that the intruder was not successful.

Logs Begin:

Apr 11 11:00:08 victim kernel: Packet log: input DENY eth0 PROTO=17
216.161.118.29:62487 Victim IP.201:161 L=72 S=0x00 I=35530 F=0x0000
T=112 (#66)

Apr 11 11:00:08 victim kernel: Packet log: input DENY eth0 PROTO=17
216.161.118.29:62487 Victim IP.204:161 L=72 S=0x00 I=34762 F=0x0000
T=112

Apr 11 12:46:13 victim kernel: Packet log: input DENY eth0 PROTO=17
attacker IP:62486 Victim IP.204:161 L=72 S=0x00 I=13940 F=0x0000
T=112

Apr 11 12:46:13 victim kernel: Packet log: input DENY eth0 PROTO=17
attacker IP:62486 Victim IP.201:161 L=72 S=0x00 I=14708 F=0x0000
T=112

[**] SNMP public access [**]
04/11-11:46:13.178242 0:E0:D0:10:EF:7F -> 0:50:4:A0:23:DD type:0x800
len:0x56
attacker IP:62486 -> Victim IP.205:161 UDP TTL:112 TOS:0x0 ID:13684
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

[**] SNMP public access [**]
04/11-11:46:13.179521 0:E0:D0:10:EF:7F -> 0:20:78:14:1F:7B type:0x800
len:0x56
attacker IP:62486 -> Victim IP.204:161 UDP TTL:112 TOS:0x0 ID:13940
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

[**] SNMP public access [**]
04/11-11:46:13.184848 0:E0:D0:10:EF:7F -> 0:C0:F0:37:D6:51 type:0x800
len:0x56
attacker IP:62486 -> Victim IP.201:161 UDP TTL:112 TOS:0x0 ID:14708
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

[**] SNMP public access [**]
04/11-11:46:13.206962 0:E0:D0:10:EF:7F -> 0:50:DA:B5:10:DF type:0x800
len:0x56
attacker IP:62486 -> Victim IP.202:161 UDP TTL:112 TOS:0x0 ID:14452
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

::::::::::::::
UDP:62487-161
::::::::::::::
[**] SNMP public access [**]
04/11-10:00:08.076910 0:E0:D0:10:EF:7F -> 0:50:4:A0:23:DD type:0x800
len:0x56
attacker IP:62487 -> Victim IP.205:161 UDP TTL:112 TOS:0x0 ID:34506
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

[**] SNMP public access [**]
04/11-10:00:08.078189 0:E0:D0:10:EF:7F -> 0:C0:F0:37:D6:51 type:0x800
len:0x56
attacker IP:62487 -> Victim IP.201:161 UDP TTL:112 TOS:0x0 ID:35530
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 ....

[**] SNMP public access [**]
04/11-10:00:08.088158 0:E0:D0:10:EF:7F -> 0:20:78:14:1F:7B type:0x800
len:0x56
attacker IP:62487 -> Victim IP.204:161 UDP TTL:112 TOS:0x0 ID:34762
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.

01 04 01 0B 02 04 03 0A 06 00 05 00 .....

[**] SNMP public access [**]
04/11-10:00:08.088483 0:E0:D0:10:EF:7F -> 0:50:DA:B5:10:DF type:0x800
len:0x56
attacker IP:62487 -> Victim IP.202:161 UDP TTL:112 TOS:0x0 ID:35274
Len: 52
30 2A 02 01 00 04 06 70 75 62 6C 69 63 A0 1D 02 0*.....public...
01 02 02 01 00 02 01 00 30 12 30 10 06 0C 2B 06 ....0.0...+.
01 04 01 0B 02 04 03 0A 06 00 05 00 .....

Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: No history available.

Identify their Techniques: A fast and automated scan of port Subseven Apocalypse trojan port 1243.

Evidence of Intent? The intent appears to be to find a vulnerable host with an open port 1243.

Evidence of Active Targeting: No, this appears to just be a part of a larger scan.

Evaluation of Information: The intruder is scanning port 1243 to see if this port is open and to then gain access to the victim through the Subseven Apocalypse trojan. I rate this unsuccessful intrusion attempt a yellow Infocon Sytem rating.

Logs Begin:

Apr 13 01:33:50 victim kernel: Packet log: input DENY eth0 PROTO=6
attacker:1261 victim.201:1243 L=48 S=0x00 I=25993 F=0x4000 T=113
SYN (#66)

Apr 13 01:33:50 www kernel: Packet log: input DENY eth0 PROTO=6
attacker:1265 victim.205:1243 L=48 S=0x00 I=27017 F=0x4000 T=113
SYN (#56)

Apr 13 01:33:50 victim kernel: Packet log: input DENY eth0 PROTO=6
attacker:1264 victim:1243 L=48 S=0x00 I=26761 F=0x4000
T=113

Logs End

Identify Hostile Individuals and Groups: A DSL account.

Identify their History: No history available.

Identify their Techniques: A fast, automated scan of UDP port 137.

Evidence of Intent? To scan for an open port 137 to gain entry to the hosts systems vulnerable, or determine whether the host is running a Windows OS or running Samba on a Unix system.

Evidence of Active Targeting: No, this could be part of a larger scan.

Evaluation of Information: This is an fast automated scan for UDP port 137 which if left open and vulnerable can gain the attacker access to the victim's drive. This scan can also tell the attacker whether or not these hosts are running a Windows Operating system or running Samba so that the attacker knows which vulnerabilities to take advantage of and what exploits to run. The Infocon system level is yellow for the need for heightened awareness.

Logs Begin:

```
Apr 14 08:31:18 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.208:137 L=78 S=0x00 I=46093 F=0x0000 T=113
Apr 14 08:31:20 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.208:137 L=78 S=0x00 I=46349 F=0x0000 T=113
Apr 14 08:31:21 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.208:137 L=78 S=0x00 I=46605 F=0x0000 T=113
Apr 14 08:31:29 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.209:137 L=78 S=0x00 I=47885 F=0x0000 T=113
Apr 14 08:31:31 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.209:137 L=78 S=0x00 I=48141 F=0x0000 T=113
Apr 14 08:31:32 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.209:137 L=78 S=0x00 I=48397 F=0x0000 T=113
Apr 14 08:31:39 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.210:137 L=78 S=0x00 I=49677 F=0x0000 T=113
Apr 14 08:31:41 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
  victim.210:137 L=78 S=0x00 I=49933 F=0x0000 T=113
```

Apr 14 08:31:42 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.210:137 L=78 S=0x00 I=50189 F=0x0000 T=113
Apr 14 08:31:53 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.211:137 L=78 S=0x00 I=51981 F=0x0000 T=113
Apr 14 08:31:54 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.211:137 L=78 S=0x00 I=52237 F=0x0000 T=113
Apr 14 08:31:56 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.211:137 L=78 S=0x00 I=52493 F=0x0000 T=113
Apr 14 08:32:04 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.212:137 L=78 S=0x00 I=53773 F=0x0000 T=113
Apr 14 08:32:05 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.212:137 L=78 S=0x00 I=54029 F=0x0000 T=113
Apr 14 08:32:07 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.212:137 L=78 S=0x00 I=54285 F=0x0000 T=113
Apr 14 08:32:17 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.213:137 L=78 S=0x00 I=56077 F=0x0000 T=113
Apr 14 08:32:19 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.213:137 L=78 S=0x00 I=56333 F=0x0000 T=113
Apr 14 08:32:20 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.213:137 L=78 S=0x00 I=56589 F=0x0000 T=113
Apr 14 08:32:28 swamprat kernel: IP fw-in deny ppp0 UDP attacker:137
victim.

Logs End