GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

*** Northcutt, a fine sample of "a day in the life of", solid analysis, put a lot of effort into severity. 82 **

This Practical is for Kirk Becker (kirk@flcu.org)

In doing this practical, I have used both resources at home and at work (we only have one machine that has any sort of intrusion detection, but will change soon). Most of these are standard incidents, with the exception of number 10. It is something I have never seen before, and cannot find any information on.

The first five events of interest come via our E-mail server at work. It is equipped with TCP Wrappers and PortSentry to help defend itself.

1.

Security Violations
=-=-=-=-=-=-=-=-=-=-=
Jan 20 08:58:10 mail in.telnetd[18701]: warning: /etc/hosts.deny, line 25: can't verify hostname: gethostbyname(machine2.dtconsulting.com) failed
Jan 20 08:58:10 mail in.telnetd[18701]: connect from 208.213.5.2
Jan 20 08:58:18 mail imapd[18705]: warning: /etc/hosts.deny, line 25: can't verify hostname: gethostbyname(machine2.dtconsulting.com) failed
Jan 20 08:58:18 mail imapd[18705]: connect from 208.213.5.2
Jan 20 08:58:18 mail imapd[18705]: imap service init from 208.213.5.2
Jan 20 08:58:19 mail imapd[18705]: Logout user=??? host=machine2.dtconsulting.com [208.213.5.2]
Jan 20 08:58:21 mail in.ftpd[18707]: warning: /etc/hosts.deny, line 25: can't verify hostname: gethostbyname(machine2.dtconsulting.com) failed

Analysis:
A interesting connection from California (according to the nslookup records). We have no relationship with this organization, yet they try to connect to 3 services on our mail server. Another interesting note would be the time - we are on Eastern time, so the connections were attempted at just before 6am Pacific time. Could we be dealing with a compromised machine on the other end?

Severity of incident: 1
Criticality - A definite connection attempt on an E-mail server - score it a 4.
Lethality - An attempt to compromise the machine, but no evidence of penetration - 3 to 4.
System Counters - An older version of a relatively secure OS, with TCP Wrappers and PortSentry - score it about a 4.
Firewall - Passing the traffic via NAT to email server - somewhere about a 2.

2.

Security Violations
=-=-=-=-=-=-=-=-=-=-=
Feb 26 13:48:14 mail ftpd[6931]: failed login from pool1-253-63.cm.starport.se [193.150.253.63], anonymous@ftp.microsoft.com
Mar 18 11:52:50 mail ftpd[18099]: failed login from cr294954-a.wlfdle1.on.wave.home.com [24.114.19.253], anonymous@ftp.microsoft.com

Analysis:
Two different attemps to log into the ftp server living on the mail server. Failed login attempt since anonymous logins are not allowed into the ftp server. It is interesting that they are both using the same email address as a login. Attempting to exploit the anonymous user on an NT box? Too bad for them we are running Linux :).

Severity of Incident: -2
Criticality - E-mail server again - 4
Lethality - I would say it is very low - 0
System - Again a relatively secure OS, TCP Wrappers and PortSentry - 4
Firewall - Passing that traffic again to the mail server - 2

3.

Mar 16 22:36:57 mail imapd[26325]: connect from 202.102.12.10
Mar 16 22:36:57 mail imapd[26325]: imap service init from 202.102.12.10
Mar 16 22:37:24 mail imapd[26325]: command stream end of file, while reading line user=??? host=[202.102.12.10]

© SANS Institute 2000 - 2005 Author retains full rights.

Analysis:
Attempting to connect to imap, which we are running. The host is an ISP in China. We have seen about 3 different attempted connects like this from Asia (once from Korea and the other from Singapore).

Severity of Incident: Probably total to about a 4.
Criticality - E-mail server - 4
Lethality - Could be an imap exploit, I doubt it is a "wrong number" from China to a small organization in Florida - 4, maybe even a 5.
System - Same E-mail server as before, TCP Wrappers and PortSentry, but it allowed the connect - 3
Firewall - NAT to the mail server - 2

4.

```
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=
Apr  8 05:14:41 mail abacus_sentry[322]: attackalert: Connect from host:
therm138.fast.u-psud.fr/193.49.25.138 to TCP port: 32773
Apr  8 05:14:42 mail abacus_sentry[322]: attackalert: Host 193.49.25.138 has
been blocked via wrappers.
Apr  8 05:14:42 mail abacus_sentry[322]: attackalert: Host 193.49.25.138 has
been blocked via dropped route.
```

Analysis:
Here we have a connect attempt to port 32773, which brings up immediate flags in PortSentry. This, though, is a port with no known attack (at least that I can find). The offending IP address is at the University of South Paris (at least what I can translate). Could be a student running a script of some sort...but what is going on at port 32773?

Severity of Incident: Probably total to about a 2.
Criticality - E-mail server - 4
Lethality - I doubt it is a "wrong number", but with no exploits that I can find, I can only score it about a 1
System - Older verion of Linux, TCP Wrappers and PortSentry, dropped connection - 4
Firewall - NAT to the mail server - 2

5.

```
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=
Apr 10 02:04:53 mail abacus_sentry[325]: attackalert: Connect from host:
clin2pool1-a56.indy.tds.net/208.170.70.57 to TCP port: 161
Apr 10 02:04:53 mail abacus_sentry[325]: attackalert: Connect from host:
clin2pool1-a56.indy.tds.net/208.170.70.57 to TCP port: 161
Apr 10 02:04:53 mail abacus_sentry[325]: attackalert: Host 208.170.70.57 has
been blocked via wrappers.
Apr 10 02:04:53 mail abacus_sentry[325]: attackalert: Host 208.170.70.57 has
been blocked via dropped route.
Apr 10 02:04:54 mail abacus_sentry[325]: attackalert: Connect from host:
clin2pool1-a56.indy.tds.net/208.170.70.57 to TCP port: 161
Apr 10 02:04:54 mail abacus_sentry[325]: attackalert: Host: 208.170.70.57 is
already blocked. Ignoring
Apr 10 02:04:58 mail abacus_sentry[325]: attackalert: Connect from host:
clin2pool1-a56.indy.tds.net/208.170.70.57 to TCP port: 161
Apr 10 02:04:58 mail abacus_sentry[325]: attackalert: Host: 208.170.70.57 is
already blocked. Ignoring
Apr 10 02:04:59 mail abacus_sentry[325]: attackalert: Connect from host:
clin2pool1-a56.indy.tds.net/208.170.70.57 to TCP port: 161
Apr 10 02:04:59 mail abacus_sentry[325]: attackalert: Host: 208.170.70.57 is
already blocked. Ignoring
```

Analysis:
Someone on a dialup ISP was attempting to connect via SNMP on our mail server. It is a port which we are not running, thus this apparently targeted attack (probably using a script, which we unfortunately do not have the port information it came from to help verify). PortSentry successfully blocked and dropped the connection.

Severity of Incident: -1.
Criticality - E-mail server - 4
Lethality - There are exploits against SNMP, but we blocked the connection and aren't running the port- 1
System - Older Version of Linux, TCP Wrappers and PortSentry, blocked

© SANS Institute 2000 - 2005 Author retains full rights.

connection - 4
Firewall - NAT to the mail server - 2

Now, I am dealing with my personal firewall at home (Norton Internet Security). It is a Windows 95 machine as patched as it can be. Lots of exploits available, and I generally have a dial-up internet connection running whenever I am home.

6.

```
04/05/2000 21:13:47 Rule "Default Block Backdoor/SubSeven Trojan" blocked
(vorlon1-i1,Backdoor-g-1).  Details:
Inbound TCP connection
Local address,service is (vorlon1-i1,Backdoor-g-1)
Remote address,service is (63.163.136.234,3967)
Process name is "N/A"
04/05/2000 21:06:21 Rule "Default Block Backdoor/SubSeven Trojan" blocked
(vorlon1-i1,Backdoor-g-1).  Details:
Inbound TCP connection
Local address,service is (vorlon1-i1,Backdoor-g-1)
Remote address,service is (63.163.136.234,3741)
Process name is "N/A"
04/05/2000 21:06:15 Rule "Default Block Backdoor/SubSeven Trojan" blocked
(vorlon1-i1,Backdoor-g-1).  Details:
Inbound TCP connection
Local address,service is (vorlon1-i1,Backdoor-g-1)
Remote address,service is (63.163.136.234,3741)
Process name is "N/A"
04/05/2000 21:06:12 Rule "Default Block Backdoor/SubSeven Trojan" blocked
(vorlon1-i1,Backdoor-g-1).  Details:
Inbound TCP connection
Local address,service is (vorlon1-i1,Backdoor-g-1)
Remote address,service is (63.163.136.234,3741)
```

Analysis:

This first incident is an attack on port 1999 (indicated by Backdoor-g-1 by NIS). This exploit is the trojan BackDoor. vorlon1 is the name of my machine. NIS recognized the signature and blocked the connection. The attack came from an ISP in Toronto, CA.

Severity of Incident: -1.
Criticality - Home PC...would be a shame to have to rebuild, but is not real critical - 2.
Lethality - Known Trojan, targeting one of my ports. - 3
System - Win 95 with as many patches Microsoft will put out, Norton IS blocked connection - 2 (being somewhat generous)
Firewall - On the system - nothing on the internet blocking the machine - 0

7.

```
03/19/2000 21:41:35 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (206.98.249.254,telnet)
03/19/2000 21:41:22 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (206.98.249.254,telnet)
03/19/2000 21:41:16 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (206.98.249.254,telnet)
03/19/2000 21:41:14 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (206.98.249.254,telnet)
```

Analysis:
Interesting, someone tried to connect to my Win 95 box via telnet. Too bad that NIS is silently blocking this port.

Severity of Incident: 1.
Criticality - Personal Home Computer - 2
Lethality - PC is not running telnet, connection was blocked silently- 1
System - Win 95 with as many patches Microsoft will put out, Norton IS blocked connection - 2 (being somewhat generous)
Firewall - On the system - nothing on the internet blocking the machine - 0

© SANS Institute 2000 - 2005 Author retains full rights.

8.

03/04/2000 15:39:44 Unused port blocking has blocked communications. Details:
Inbound TCP connection
Remote address,local service is (209.215.8.156,27374)
03/04/2000 15:39:41 Unused port blocking has blocked communications. Details:
Inbound TCP connection
Remote address,local service is (209.215.8.156,27374)

Analysis:
This is a search to see if I have a trojan on my PC (in this case, Sub Seven). The virus software says I do not have the trojan, but Norton Internet Security does not have that information in their database. The connection was being attempted to an unused port, so it was silently dropped. They are definitely looking for something.

Severity of Incident: 3.
Criticality - Home computer - 2
Lethality - The attempt is to see if I have a known trojan, but the connection is dropped- 3
System - Win 95 with as many patches Microsoft will put out, Norton IS blocked connection - 2 (being somewhat generous)
Firewall - On the system - nothing on the internet blocking the machine - 0

9.

03/01/2000 23:58:10 Rule "Default Block NetBus Trojan" blocked
(216.78.87.114,NetBus). Details:
Inbound TCP connection
Local address,service is (216.78.87.114,NetBus)
Remote address,service is (216.78.38.82,11111)
Process name is "N/A"
03/01/2000 23:57:58 Rule "Default Block NetBus Trojan" blocked
(216.78.87.114,NetBus). Details:
Inbound TCP connection
Local address,service is (216.78.87.114,NetBus)
Remote address,service is (216.78.38.82,11111)
Process name is "N/A"
03/01/2000 23:57:52 Rule "Default Block NetBus Trojan" blocked
(216.78.87.114,NetBus). Details:
Inbound TCP connection
Local address,service is (216.78.87.114,NetBus)
Remote address,service is (216.78.38.82,11111)
Process name is "N/A"
03/01/2000 23:57:49 Rule "Default Block NetBus Trojan" blocked
(216.78.87.114,NetBus). Details:
Inbound TCP connection
Local address,service is (216.78.87.114,NetBus)
Remote address,service is (216.78.38.82,11111)
Process name is "N/A"

Analysis:
Ah...just have to love those trojan sweeps. This time, someone is looking to connect to NetBus. These are definitely crafted packets (since the port does not change in the remote address), probably some sort of script. Interesting thing is that they use the same regional ISP I do, but at a dial-up connection in North Carolina.

Severity of Incident: 3.
Criticality - Home computer - 2
Lethality - The attempt is to see if I have a known trojan, but the connection is dropped- 3
System - Win 95 with as many patches Microsoft will put out, Norton IS blocked connection - 2 (being somewhat generous)
Firewall - On the system - nothing on the internet blocking the machine - 0

10.

03/11/2000 0:21:35 Unused port blocking has blocked communications. Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:21:25 Unused port blocking has blocked communications. Details:
Inbound TCP connection

© SANS Institute 2000 - 2005 Author retains full rights.

```
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:21:19 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:21:14 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:20:03 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:19:53 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:19:48 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/11/2000 0:19:43 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (208.29.104.138,13223)
03/07/2000 21:40:05 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:39:53 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:39:47 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:39:44 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:37:58 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:37:46 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.66.34.224,13223)
03/07/2000 21:22:14 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:22:02 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:56 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:54 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:53 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:47 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:44 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:06 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:21:03 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (209.252.88.95,13223)
03/07/2000 21:17:39 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:17:27 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:17:21 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:17:18 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:15:34 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:15:22 Unused port blocking has blocked communications.  Details:
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:15:16 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:15:13 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:13:28 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:13:16 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:13:12 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:13:09 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:11:23 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:11:11 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:11:05 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
03/07/2000 21:11:03 Unused port blocking has blocked communications.  Details:
Inbound TCP connection
Remote address,local service is (12.77.88.91,13223)
```

Analysis:
This set of incidents really have me intrigued. I have not seen any more of these detects anywhere since the one week that this is occurred. The incidents are coming from various ISP's, a couple large names as a matter of fact. I cannot tell if these are spoofed IP addresses, but one in particular (209.252.88.95) has probed my machine before looking for a trojan. The port that they are trying to connect to does not seem to be listed on any database anywhere as a trojan port, there do not seem to be any known exploits against that port anywhere (not just Win 9x). Whitehats, SecurityFocus, SANS, even Phrack and L0pht have no information about anything dealing with this port. I am wondering if anyone else has seen anyone trying to connect to this port. Like I mentioned earlier, this has only happened during one week timeframe, and I have not seen hide nor hair of this either at work or at home since.

These connections seem to come in groups of 5 to 8 in about a 45 second time frame, a wait of about 30 seconds to up to 2 minutes, and then another round.

Severity of Incident: somewhere about a 3.
Criticality - Home PC - 2
Lethality - Hard to tell with this one. Norton Internet Security blocked this connection silently since it is set to do so with the unused ports. What is going on with port 13223? - 3
System - Win 95 with as many patches Microsoft will put out, Norton IS blocked connection - 2 (being somewhat generous)
Firewall - On the system - nothing on the internet blocking the machine - 0

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: April 25th, 2017

Upcoming Training

SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, Switzerland	May 15, 2017 - May 20, 2017	Live Event
Mentor Session - SEC503	Oceanside, CA	May 29, 2017 - Jun 29, 2017	Mentor
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio Fall 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
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
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego Fall 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 OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced