Global Information Assurance Certification Paper

Introduction:

This work is for completion of assignment from the GIAC Intrusion and Detection Curriculm, Practical Assignment for SNAP San Jose, May 8-13, 2000. It attempts to meet the practical objective of describing 10 detect of suspicious traffic. It was generated through these Internet access points.

1. Home computer linked to the Internet through DSL broadband services.
2. Network managed for a non-profit, all volunteer organization dedicated to providing tutorial services to secondary age students.

It has been an important learning experience. The importance of due vilagence was brought home quickly. I have used personalized firewalls since before my connection to broadband service. I have always been amazed at the number of alerts generated at my always-on connection. Attending the SANS training classes has brought on to me a new understanding of what these attempts have really mean. I know look at these alerts under a new light. I now look for patterns, source and destination ports more than I do IP address. I understand why packages are crafted, and some signs to look for. I also now fear security compromises and understand they are only another CERT advisory away. This has also been a humbling experience. I fully believe my sloppy administration habits at the non-for profit network has left some vulnabilities available. Why hadn't I turned of all these unneeded services, and maintained patch level on cgi-bin applications running on the web server. These have allowed a web server to appear to be a conduct of some type of traffic I am still trying to identify. I know better than that, after all I am suppose to be a Security professional. I fell into the trap that there was nothing important enough for any one to mess with. Opening unneeded services helped to advertise a weakly secured machines and taught me an important lesson, "Any computer connected to the Internet is important, just because it is connected". It is capability of being misuded by others if you are not careful.

These report is broken in two several detects grouped together based on traffic exploit patterns. Information is taken from logs files. Log files were created or enhanced by using the following.

1. Home network consists of a Microsoft based computer protected by Network Ice, BlackIce Defender, (http://www.networkice.com/). Logs are taken by enabling the evidence logging in the BlackIce settings. Evidence collected is the sniffed packet from the wire that caused blocking filter to fire. These logs have helped me to differentiate between the available protection options available. High settings act like a firewall drop and do not acknowledge scans, while lower ones act like the reject firewall rule and contribute to reconanise efforts by providing information back to attacker. The logs are then opened using the capture program from SpyNet http://www.eeye.com/html/Products/iris.html) and then saving the data in a columnized text output. Time values are relative to start of capture.
2. Non-for profit network is a mixture of Linux, Windows 9x and NT computers. Linux provides web hosting and DNS services. Desktop, file sharing, printers and authentication methods are Microsoft based. Reports provided are strictly Linux based. Basic log information is based on the syslogd service. Reports have been enhanced with the supplemental use of tool such as logchecker (http://www.psionic.com/abacus/logcheck/). It is used to group important messages and mail important information back for inspection. Protection methods were enhanced by using PortSebtry (http://www.psionic.com/abacus/portsentry/); it truly is a great product. It not only alerts you through the syslogd facility to unauthorized access to ports, but also will use tcp wrappers and the route command to make do0r rattlers disappear. Deeper package inspection is handle with ippl logs (http://pltplp.net/ippl/). It allows for logging important packet signatures. Of course the old Unix stand by tcpdump Lawrence Berkeley Labs, is available and as I get more concerned with traffic seen, I have start to learn it use.

I hope this report is as useful to those who read it, as it was I developing it. It has made me pull out the Stevens Bible, Volume one to get a better understanding of port usage, and what traffic is expected and which is darn right strange. If you like correlations, there are several in this report. Correlations are available from other GIAC reports and system logs. If you like to see traces, take your pick, I have numerous traces available. If you like mysteries, then please help me understand what is going on with all of the use of the ident or auth service request seen on port 113. I have done some digging, but it show they is still a lot

left for me to learn. But if you reminder one thing from this report, let it be this, “Always utilize and read your logs”. You can never have enough.

Enjoy!

Harrison C. May

Detect #1 (Port 111 or SUNRPC Scan Detects)
The following information is taken from (http://advice.networkice.com/advice/Intrusions/2003105).
Summary: An intruder has attempted to access the Sun RPC (rpcbind, portmapper) service on your system. This is probably during a sweep of millions of machines on the Internet, and is probably not targeting your computer in particular

(1A) Generated by BlackIce Defender from Erol's Internet Services (NETBLK-EROLSBLK-5)

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
0	0:0:54392:550	IP	TCP->SUNRPC	216.164.126.3	home.net	111	111	1654832355	1327542883	54
1	0:0:54392:550	IP	TCP->SUNRPC	216.164.126.3	home.net	111	111	2084709	480568333	54

======

(1B-1a) Name Server ippl log fr from @Home Network (NETBLK-HLNDPK1-IL-1)
Log attained using ippl
Jun 6 03:32:38 sunrpc connection attempt from Sunrpc-Probber.com[24.11.38.220] (24.11.38.220:4198->nane-server.edu:111)
Jun 6 03:32:39 sunrpc connection attempt from Sunrpc-Probber.com[24.11.38.220] (24.11.38.220:673-> nane-server.edu:111)
Jun 6 03:32:39 sunrpc connection closed from Sunrpc-Probber.com [24.11.38.220] (24.11.38.220:673-> nane-server.edu:111)
Jun 6 03:32:39 sunrpc connection closed from Sunrpc-Probber.com [24.11.38.220] (24.11.38.220:4198-> nane-server.edu:111)

(1B-1b) Name Server PortSentry Response from @Home Network (NETBLK-HLNDPK1-IL-1
Jun 6 03:32:38 ns1 portsentry[1088]: attackalert: Connect from host: Sunrpc-Probber.com/24.11.38.220 to TCP port: 111
Jun 6 03:32:38 ns1 portsentry[1088]: attackalert: Host 24.11.38.220 has been blocked via wrappers with string: "ALL: 24.11.38.220"
Jun 6 03:32:39 ns1 portsentry[1088]: attackalert: Connect from host: Sunrpc-Probber.com/24.11.38.220 to TCP port: 111
Jun 6 03:32:39 ns1 portsentry[1088]: attackalert: Host: 24.11.38.220 is already blocked. Ignoring

(1B-2) Web Servers ippl Log from from @Home Network (NETBLK-HLNDPK1-IL-1
Jun 6 03:35:43 port 111 connection attempt from Sunrpc-Probber.com[24.11.38.220] (24.11.38.220:4180->web.edu:111)
======

(1C) Web Server ippl Log from UTILNET-2 Utilnet is an Internet Service Provider based in France
May 20 15:21:16 port 111 connection attempt from unknown@195.154.202.153 (195.154.202.153:2666->web.edu:111)
May 20 15:21:16 port 111 connection attempt from unknown@195.154.202.153 (195.154.202.153:2666->web.edu:111)
May 20 15:21:17 port 29599 connections closed from 195.154.202.153 (195.154.202.153:113-> web.edu:29599)

(1D) Generated by BlackIce Defender from CAIS Internet (NETBLK-CAIS-CIDR7)

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
15	0:0:52840:550	IP	TCP->SUNRPC	63.216.49.132	home.net	4847	111	993165257	0	74
16	0:0:52840:550	IP	TCP->SUNRPC	63.216.49.132	home.net	4847	111	993165257	0	74

Source of Traces

Detect 1A	Data collected from Home computer (home.net) that has a DSL connection.
Detect 1B-1a	Data collected from Education name server (name.edu) that is running Linux
Detect 1B-1b	Data collected from Education name server (web.edu) that is running Linux.
Detect 1B-2	Data collected from Education web server (web.edu) that is running Linux.
Detect 1C	Data collected from Education web server (web.edu) that is running Linux.
Detect 1D	Data collected from Home computer (home.net) that has a DSL connection.

Detects were generated by

Detect 1A	Network Ice Black Ice Defender http://www.networkice.com/.
Detect 1B-1	Data collected using Unix ippl logging facility http://pltplp.net/ippl/ Grep command used on IP address found in SANS report.
Detect 1B-2	Unix Port Sentry http://www.psionic.com/abacus/portsentry/.
Detect 1B-2a	Unix Port Sentry http://www.psionic.com/abacus/portsentry/
Detect 1C	Data collected using Unix ippl logging facility http://pltplp.net/ippl/. Grep used on log for IP address listed in a GIAC report..
Detect 1D	Data collected from Home computer (home.net) that has a DSL connection.

Probability that source address was spoofed

Detect 1A-D	Traces were probably not spoofed addresses. Two are examples of the dangers of broadband. The others are scans that had correlations. All had one thing in common port 111 or potmapper, sunrpc. Two of them are too wide see to anything expect data mining missions. If these are not a hacked machine then a owner is hacking.

Description of Attack

Detect 1A&D	BlackIce reports a tcp scan for the sunrpc port.
Detect 1B	Scan covered my portion of a Class C network. Hit two machines in two minutes, This detect was attributed to Tod Kohl's contribution at SANS (http://www.sans.org/y2k/061000.htm). Same user has entries in both Web and Name-Server attempting to access Port 111. Appearing to be running wide and straight for port 111.
Detect 1C	Port 113 appears to be in too many log entries. This port exchange looked strange to me. I discovered it because of the port action, Port open 2666-111 closed 113-29599. I believe we have a crafted package here. What it hidden inside of this packet, or did my web server responsed to a service I am not aware of?

Description of Attack

The following information is taken from
(http://advice.networkice.com/advice/Intrusions/2003105)
Summary An intruder has attempted to access the Sun RPC (rpcbind, portmapper) service on your system. This is probably during a sweep of millions of machines on the Internet, and is probably not targeting your computer in particular.

These three attacks are examples of for machines scanning for machines running the service, SUNRPC. Information on this service vulnerability is discussed in the CERT® Advisory CA-99-08 Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd (http://www.cert.org/).

Attack Method

Detect 1A&D	This is probably during a sweep of machines on the broadband metwork,, I am attached to..
Detect 1B	Wide scan that crossed multiple networks. See correlation.
Detect 1C	Port scans for port 111 across multiple networks. See correlation. How do you open a port connection with one port and then close a different port. Is this the pattern of a crafted packet?

Correlation

Detect 1A&D	None.
Detect 1B	This detect was attributed to Tod Kohl's contribution at SANS (http://www.sans.org/y2k/061000.htm).
.Detect 1C	Sean Brown Correlation an IP scans from France. (http://www.sans.org/y2k/052500.htm

Evidence of active targeting

Detect 1A&D	Only looked for port 111.
Detect 1B	Definitely an example of active scanning or reconnaissance work. Multiple machines were probed at my site and Correlation proves other sites were affected
Detect 1C	Sean Brown Correlation an IP scan from France. (http://www.sans.org/y2k/052500.htm). Strange port combination appeared. He also sees port 2666. Little too strange.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 1A	(3 + 4) – (5 + 5) = -3
Detect 1B	(5 + 4) – (5 + 2) = 2
Detect 1C	(5 + 4) – (3 + 2) = 4
Detect 1D	(3 + 4) – (3 + 2) = -3

Defensive Recommendation

Detect 1A&D	BlackIce to the rescue.
Detect 1B	PortSentry behaved nicely.
Detect 1C	IPPL logs are great for looking at Ip addresses and port numbers. PortSentry could have actually blocked.

Multiple Choice Test Question

Match Question with Choices

1. Which tool actively blocks computer based on port 111 access
2. Which tool is used to display port number.
3. Which tool uses relative time as a timestamp.
4. What service is the mentioned CERT report concerning.

Choices

A	BlackIce
B	IPPL Logging
C	Sunrpc
D	Port Sentry

Answers 1-1-D 1-2-B 1-3-A 1-4-D

Detect #2 (Port 1080 Socks or WinGate Scan Detects)
The following information is taken from
(http://advice.networkice.com/advice/Reference/Networking/SOCKS/default.htm)
Most scans for port 1080 are actually looking for WinGate, a popular firewall/proxy for Windows. In theory, SOCKS should only be visible from the internal side of the server, but not from the Internet. Hackers will frequently probe to see if SOCKS is visible from the other side. If that is the case, they can attack your internal network, or almost as bad, launch attacks on other Internet sites from your machine

(2A) Port Sentry response on web.edu
Active System Attack Alerts
=-=-=-=-=-=-=-=-=-=-=-=-=-=
May 24 02:28:51 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:28:51 web.edu portsentry[5730]: attackalert: Host 4.34.128.221 has been blocked via wrappers with string: "ALL: 4.34.128.221"
May 24 02:28:51 web.edu portsentry[5730]: attackalert: Host 4.34.128.221 has been blocked via dropped route using command: "/sbin/route add -host 4.34.128.221 reject"
May 24 02:28:52 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:28:52 web.edu portsentry[5730]: attackalert: Host: Win-Gate-Scan.net/4.34.128.221 is already blocked Ignoring
May 24 02:28:58 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:28:58 web.edu portsentry[5730]: attackalert: Host: Win-Gate-Scan.net/4.34.128.221 is already blocked Ignoring
May 24 02:29:08 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:29:08 web.edu portsentry[5730]: attackalert: Host: Win-Gate-Scan.net/4.34.128.221 is already blocked Ignoring
May 24 02:29:11 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:29:11 web.edu portsentry[5730]: attackalert: Host: Win-Gate-Scan.net/4.34.128.221 is already blocked Ignoring
May 24 02:29:17 web.edu portsentry[5730]: attackalert: SYN/Normal scan from host: Win-Gate-Scan.net/4.34.128.221 to TCP port: 1080
May 24 02:29:17 web.edu portsentry[5730]: attackalert: Host: Win-Gate-Scan.net/4.34.128.221 is already blocked Ignoring

(2B) Generated by BlackIce Defender on 30May2000 from UUNET Technologies, Inc. (NETBLK-UUNET63

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
0	0:0:51312:550	IP	TCP->SOCKS	home.net	63.96.48.68	1080	1103	0	2726821783	54
1	0:0:51312:550	IP	TCP->SOCKS	home.net	63.96.48.68	1080	1103	0	2726821783	54
2	0:0:51312:550	IP	TCP->SOCKS	home.net	63.96.48.68	1080	1103	0	2726821783	54

Source of Traces
Detect 2A Data collected from Education web server (web.edu) that is running Linux.
Detect 2B Data collected from Home computer (home.net) that has a DSL connection.

Detects were generated by
Detect 2A Unix Port Sentry. Detailed information of product is located at

http://www.psionic.com/abacus/portsentry/

Detect 2B Network Ice Black Ice Defender. Detailed information of product is located at (http://www.networkice.com/)

Probability that source address was spoofed

Detect 2A This was probably not a spoofed address. The successful user probably would have used me as a proxy.

Detect 2B This was probably not a spoofed address. The successful user probably would have used me as a proxy

Description of Attack

The following information is taken from (http://advice.networkice.com/advice/Intrusions/2003017)

Someone is scanning your system to see if it is running SOCKS. This may be a hacker that desires to "bounce" traffic through your system at other people. It may also be a chat server trying to determine if someone is indeed bouncing through your system to chat anonymously. The problem with SOCKS and products like WinGate is that it isn't picky about the source and destination. Just as it allows internal machines access to the Internet, it possibly will allow Internet machines to access the internal home network. Most importantly, it may allow a hacker access to other Internet machines through your system. This allows the hacker to hide his/her true location. The attacks against the victim appear to come from your machine, not from the real hacker. The ability to hide their tracks like this is important to hackers. Therefore, hackers scour the Internet religiously looking for systems they can bounce their attacks through. This intrusion signature indicates that somebody scanned your system looking for SOCKS, but probably did not find it.

Detect 2A Attacker scans IP address usually using a tool.

Detect 2B Attacker scanned home.net or more like my broadband address space looking for a computer to use as a proxy.

Correlation

Detect 2A None

Detect 2B None

Evidence of active targeting

Detect 2A Only looked for one port.

Detect 2B Only looked for one port.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 2A (5 + 4) – (5 + 2) = 2

Detect 2B (3 + 4) – (5 + 5) = -3

Defensive Recommendation

Detect 2A Defense on machine worked as expected. Port Sentry uses the route command to drop future packages from this site. It also documented attack and response by placing entry in syslogd

Detect 2B Computer is using BlackIce Defender for protection. The trace shows that BlackIce responded to attacker before it actually starting blocking intruder. This is due to the protection setting in BlackIce. Further communication with this host will be blocked

Multiple Choice Test Question

Match Question with Choices

1. Which tool actively looks for WinGate
2. Which tool is actively changes networking information on host.
3. Which tool allows a response before responding.
4. What service allowing for proxing.

Choices

A	BlackIce
B	Socks
C	Sunrpc
D	Port Sentry

Answers 2-1-D 2-2-D 2-3-A 2-4-B

Detect #3 (Scan PC AnyWhere)
The following information is taken from
(http://advice.networkice.com/advice/Intrusions/2003012/default.htm)
A hacker may be scanning your system to see if the PCANYWHERE service is available on your system. Sometimes this is done in preparation for a future attack, or sometimes it is done to see if your system might be susceptible to attack.

(3A) BlackIce Generated by BlackIce Defender on 12Jun2000 from Unified Building Science Engineering Inc (NETBLK-SBCIS54469)

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
0	0:0:2696:551	IP	UDP	208.189.89.57	home.net	3864	5632	---	---	44

(3B) BlackIce Generated by BlackIce Defender on 13Jun2000 from My Broadband Provider

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
3	0:0:51312:550	IP	UDP	PCScan.home	home.net	1026	22	---	---	44
4	0:0:51312:550	IP	UDP	PCScan.home	home.net	1028	5632	---	---	44
5	0:0:51312:550	IP	UDP	PCScan.home	home.net	1028	22	---	---	44

Source of Traces
- Detect 3A: Data collected from Home computer (home.net) that has a DSL connection.
- Detect 3B: Data collected from Home computer (home.net) that has a DSL connection

Detects were generated by
- Detect 3A: Network Ice Black Ice Defender. Detailed information of product is located at (http://www.networkice.com/)
- Detect 3B: Network Ice Black Ice Defender. Detailed information of product is located at (http://www.networkice.com/)

Probability that source address was spoofed
- Detect 3A-B: This was probably not a spoofed address. Someone looking for one of his or her machines to control or an unprotected one to exploit.

Description of Attack
An example of scans using UDP for PC AnyWhere

Correlation
- Detect 3A-C: None

Evidence of active targeting
- Detect 3A: Users looking for PC Anywhere servers

Severity

Defensive Recommendation
- Detect 3A-3C: BlackIce to the rescue after he allows a reply.

Multiple Choice Test Question
(Critical + Lethal) – (System + Net Countermeasures) = Severity
- Detect 3A: (3 + 5) – (5 + 4) = -1
- Detect 3B: (3 + 5) – (5 + 4) = -1

Match Question with Choices

3. These example show PC AnyWHere scans using what protocol?

Choices

A TCP
B IP
C UDP
D ICMP

Answers 3C

Detect #4 Port 261 Attempts for nearly one hour

(4A) Web Server ippl log on web.edu from San Diego City Schools (NET-SDCS)
May 24 14:56:46 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34814-web.edu:261)
May 24 14:56:56 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34825->web.edu:261)
May 24 14:57:01 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34843->web.edu:261)
May 24 14:57:06 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34865->web.edu:261)
May 24 14:57:11 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34884->web.edu:261)
May 24 14:57:16 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:34904->web.edu:261)

--SNIP—

May 24 15:41:02 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46300->web.edu:261)
May 24 15:41:07 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46323->web.edu:261)
May 24 15:41:12 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46342->web.edu:261)
May 24 15:41:17 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46361->web.edu:261)
May 24 15:41:22 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46382->web.edu:261)
May 24 15:41:27 port 261 connection attempt from port261@fw-sandi.net [165.24.5.66] (165.24.5.66:46403->web.edu:261)

Source of Traces

Detect 4A	Data collected from Education web server (web.edu) that is running Linux.

Detects were generated by

Detect 4A	Data collected using Unix ippl logging facility information at (http://pltplp.net/ippl/) . Log then grepped for port to build list of ports accessed. This entry appeared suspicious due to the number of probes seen and the quantity of 6 involves.

Probability that source address was spoofed

Detect 4A	Doesn't appear to be spoofed IP address. Really need to have more packet details to investigate further. I wonder what flags are set. Packets increment nicely. Some tool is running somewhere. No port-closed connections noticed.

Description of Attack

Detect 4A	Attacker repeat tried to access port 261 on my Unix web server. Not sure what they where looking for. I have no services available at that port. Multiple sites that list common ports have no information available about port 261. I checked at the following web sites. RFC 1700 states this is an unassigned port. Really need to have more packet detail to investigate further. I wonder what flags are set. Is this a DoS or am I being used to created a DoS? Packets increment nicely. No port-closed connections noticed.

Correlation

Detect 4A	This is a prime example of ensuring that you enter the correct information when doing a whois query. I previously spent 16 years working for DOE and traveled

many times to visit the Sandia labs. Notice the detect came from sandi.net, not sandia.net Here is a little history of my embarrassment from asking the domain administrator of sandia.net to investigate

From: Harrison C. May
To: schavez@sandia.net ; postmaster@sandia.net
Sent: Tuesday, June 06, 2000 2:41 AM
Subject: Unusual Activity from your site
Dear Sir attached is log information from activity detected from you site on May 24, CDT. A machine on your site made repeated connection attempts every 5-10 seconds to port 261. I have no services running at that port which makes the access even stranger.

And their reply

Dear sir,
We are sandia.net NOT **"sandi.net"** as indicated below,
Thanks
Sal

Finally I send information to the right administrator

Harrison,

Thank you for the log excerpts. I will attempt to look into further, unfortunately the source address is likely a NAT address behind our firewall that is not fully logged. Please notify me if you get further log entries from our class B 165.24.x.x.

Grant Gutstadt - security administration
san diego city schools - technology support services
gutstadt@mail.sandi.net - (619) 725-7483

Evidence of active targeting

Detect 4A	Port is hit hard. Makes me curios what is really going on. Wish I had more logging capability.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 4A	(5 + 2) – (3 + 2) = 2

Defensive Recommendation

Detect 4A	Port Sentry would be nice. Really calls for a network sensor looking for flag settings to check DoS

Multiple Choice Test Question
Detect 4

Match Question with Choices
4. Port 261 houses what services

Choices

A	Unassigned reserved number
B	Pop3
C	SUNrpc
D	echo

Answers 4-A

Detect #5 (Port 1243 Sub Seven)
The following information is taken http://advice.networkice.com/advice/Intrusions/2003105/default.htm
Somebody has tried to access your machine with the "Sub Seven Trojan Horse" and failed

(5A) ippl log on web.edu from Internet Direct Canada Inc. (NETBLK-NETBLK-IDCA-3
Apr 30 14:40:35 port 1243 connection attempt from Sub Seven.probe[216.154.47.137]
(216.154.47.137:4297->web.edu:1243)

(5B) BlackIce Generated by BlackIce Defender on 10Jun2000 from HSE (Sympatico) (NETBLK-HSE2000-CA)

No	Timestamp	Type	Protocol	IP src	IP dest	Port src	Port dest	SEQ	ACK	Size0
4	0:0:51312:550	IP	TCP	home.net	64.228.64.178	1243	4785	0	8749674	54
5	0:0:51312:550	IP	TCP	home.net	64.228.64.178	1243	4785	0	8749674	54

(5C) BlackIce Generated by BlackIce Defender from Home Network (NETBLK-RDC1-MI-4)

No	Timestamp	Type	Protocol	IP src	IP dest	Port-src	Port-dest	SEQ	ACK	Size0
7	0:0:54392:550	IP	TCP	home.net	24.10.57.144	27374	3692	0	21809935	54
8	0:0:54392:550	IP	TCP	home.net	24.10.57.144	27374	3692	0	21809935	54
9	0:0:54392:550	IP	TCP	home.net	24.10.57.144	27374	3692	0	21809935	54
10	0:0:54392:550	IP	TCP	home.net	24.10.57.144	27374	3692	0	21809935	54

(5D) BlackIce Generated by BlackIce Defender on 13Jun2000 from JPNIC-NET-JP

No	Timestamp	Type	Protocol	IP src	IP dest	Port-src	Port-dest	SEQ	ACK	Size0
6	0:0:51312:550	IP	TCP	210.189.72.12	home.net	16513	27374	2081904259	0	58
7	0:0:51312:550	IP	TCP	210.189.72.12	home.net	16513	27374	2081904259	0	58
8	0:0:51312:550	IP	TCP	210.189.72.12	home.net	16513	27374	2081904259	0	58
9	0:0:51312:550	IP	TCP	210.189.72.12	home.net	16513	27374	2081904259	0	58

Source of Traces

Detect 5A	Data collected from Education web server (web.edu) that is running Linux
Detect 5B-D	Data collected from Home computer (home.net) that has a DSL connection.

Detects were generated by

Detect 5A	Data collected using Unix ippl logging facility http://pltplp.net/ippl/ Grep command used on port 1243.
Detect 5B-D	Network Ice Black Ice Defender. Detailed information of product is located at (http://www.networkice.com/)

Probability that source address was spoofed

Detect 5A-D	This was probably not a spoofed address. Someone looking for one of his or her machines to control or an unprotected one to exploit.

Description of Attack

The following information is taken
http://advice.networkice.com/advice/Intrusions/2003105/default.htm.

> This is a common intrusion detected on the Internet, resulting from hackers looking for systems who might have been compromised with this program. It appears that you *haven't* been compromised, and that the hacker has gone away.
> A Trojan program is one that has some subversive purpose other than what it looks like One of the favorite hacker techniques is to send these programs to people in the hopes they will be fooled into running them. Typical Trojans are those that steal passwords, install a virus, reformat your hard-disk, and so forth.
>
> A particular popular class of Trojans are the Remote Access Trojans. These are programs that provide the hacker complete remote control over your machine. The problem for that hacker is that while they can often send you such Trojans via e-mail, chat, or news programs, they often don't know where on the Internet you are located. For example, they can tell from your e-mail that you use a certain ISP, but they don't know your current IP address. Therefore, if they think they've fooled you into running their program, they must then scan the entire ISP's range for you.
>
> The flip-side to this means that if the hacker isn't after you, you will still see their scans as they search for their other victims. Likewise, the hacker may hope that some other hacker has hoodwinked you into running this Trojan. This means the hacker may be looking for *anybody* who might be compromised.

Correlation

Detect 5A-D	None

Evidence of active targeting

Detect 5A-D	Known sub7 ports were scanned for. Only activity to hosts from this IP address.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 5A	(5 + 3) – (4 + 2) = 2
Detect 5B	(3 + 5) – (5 + 3) = 0
Detect 5C	(3 + 5) – (5 + 3) = 0
Detect 5D	(3 + 5) – (5 + 4) = -1

Defensive Recommendation

Detect 5A	Port Sentry would have been nice to have stop probe and drop the offending address into a routing black hole.
Detect 5B-D	BlackIce to the rescue after he allows a reply except in attack 5D. Protection level moved from Cautious to Nervous, which appears to stop reply from going back.

Multiple Choice Test Question

Detect 5

Match Question with Choices

5. Sub Seven utilizes what protocol?

Choices

A	TCP
B	IP
C	UDP
D	ICMP

Answers 5A

Detect # 6 (Port 98 LinuxConf attempt)

(6A)) ippl log on web.edu from (CHANNELI LG) InterNet Inc Korea
May 30 16:29:11 linuxconf connection attempt from unknown@210.112.192.74 (210.112.192.74:3875-> web.edu:98)
May 31 03:44:54 linuxconf connection attempt from unknown@210.112.192.74 (210.112.192.74:4670-> web.edu:98)

Source of Traces

Detect 6A Data collected from Education web server (web.edu) that is running Linux

Detects were generated by

Detect 6A Data collected using Unix ippl logging facility http://pltplp.net/ippl/ Grep command used on port IP address.

Probability that source address was spoofed

Detect 6A This was probably not a spoofed address. Someone looking for Linxconf.

Description of Attack

Exploiting the potential linuxconf hole many scans are looking for this port availability.

The following information was taken for http://advice.networkice.com/advice/Exploits/Ports/98/default.htm This port was assigned to a service called "TAC News", but in the real world it has been used for the HTTP daemon included as part of the "linuxconf" package for remote administration
The following information is taken http://lwn.net/1999/1223/a/linuxconfresponse.html.

So this could be a false alarm, but, many people have reported that service 98 is scanned, so I would guess that there a reason for that. If the exploit is possible, the solution is to disable "linuxconf network access" using the supplied check-box. Default linuxconf installations are safe.

Correlation

Detect 6A Detect attributed to Computer and Network Security Officer, The University of Auckland, New Zealand http://www.sans.org/y2k/053000-1100.htm. Tod Kohl from http://www.sans.org/y2k/060100.htm. Sean Brown's from http://www.sans.org/y2k/060100-1400.htm. Daniel B. Holzman from http://www.sans.org/y2k/060300.htm

Evidence of active targeting

Detect 6A IP address was seen in multiple GIAC reports looking for port 98. It probe my web server twice, two days in a row. Not sure why he came back. No linuxconf services provided on this machine.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 6A (5 + 5) – (4 + 2) = 4

Defensive Recommendation

Detect 6A Port Sentry would have been nice to have stop probe and drop the offending address into a routing black hole.

Multiple Choice Test Question

Detect 6

Match Question with Choices

6. Port 98 allows for running what services?

Choices

A echo

B Pop3
C Linuxconf
D Sunrpc

Answers 6C

Detect #7 (HTTP masked Portscan, Socks, FTP Bounce?)
This information is from
http://advice.networkice.com/advice/Underground/Hacking/Methods/Technical/Port_Scan/default.htm
Port Scanning is one of the most popular reconnaissance techniques hackers use to discover services they can break into. A potential victim computer runs many 'services' that listen at well-known 'ports'. By scanning which ports are available on the victim, the hacker finds potential weaknesses that can be exploited

(7A) ippl log on web.edu Centre Interuniversitaire de Calcul de Toulouse (NET-UNITOUL)
May 22 07:45:13 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1645-> web.edu:80)
May 22 07:45:18 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1646-> web.edu:80)
May 22 07:45:22 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1647-> web.edu:80)
May 22 07:45:23 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1648-> web.edu:80)
May 22 07:45:27 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1646-> web.edu:80)
May 22 07:45:30 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1647-> web.edu:80)
May 22 07:45:31 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1648-> web.edu:80)
May 22 07:45:31 port 10993 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10993)
May 22 07:45:31 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1645-> web.edu:80)
May 22 07:45:36 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1648-> web.edu:80)
May 22 07:45:36 port 10995 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10995)
May 22 07:45:36 port 10996 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10996)
May 22 07:45:36 port 10995 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10995)
May 22 07:45:36 port 10997 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10997)
May 22 07:45:36 port 10998 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10998)
May 22 07:45:36 port 10999 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10999)
May 22 07:45:36 port 10998 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10998)
May 22 07:45:36 port 10999 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10999)

-SNIP –

May 22 08:00:04 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1674-> web.edu:80)
May 22 08:00:12 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1676-> web.edu:80)
May 22 08:00:17 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1679-> web.edu:80)
May 22 08:00:22 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1677-> web.edu:80)
May 22 08:00:23 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1680-> web.edu:80)
May 22 08:00:23 port 11186 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113->

web.edu:11186)
May 22 08:00:37 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1678->
web.edu:80)
May 22 08:00:38 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1681->
web.edu:80)
May 22 08:00:38 port 11187 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113->
web.edu:11187)
May 22 08:02:01 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1679->
web.edu:80)
May 22 08:02:06 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1680->
web.edu:80)

(7B-1) ippl log on web.edu from PARADISE-NZ-WEBBINF
Apr 21 21:05:51 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:2953->web.edu:80)
Apr 21 21:06:17 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3630->web.edu:80)
Apr 21 21:06:18 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3677->web.edu:80)
Apr 21 21:06:20 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3678->web.edu:80)
Apr 21 21:06:22 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3679->web.edu:80)
Apr 21 21:06:23 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3756->web.edu:80)
Apr 21 21:06:25 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:3855->web.edu:80)

(7B-2) ippl log on web.edu from PARADISE-NZ-WEBBINF
Apr 26 17:29:11 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42236->web.edu:80)
Apr 26 17:29:13 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42236->web.edu:80)
Apr 26 17:29:15 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42294->web.edu:80)
Apr 26 17:29:18 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42295->web.edu:80)
Apr 26 17:29:20 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42296->web.edu:80)
Apr 26 17:29:26 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42294->web.edu:80)
Apr 26 17:29:29 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42295->web.edu:80)
Apr 26 17:29:29 port 25748 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:25748)
Apr 26 17:29:29 port 25749 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:25749)
Apr 26 17:29:29 port 25749 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:25749)
Apr 26 17:29:29 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42294->web.edu:80)
Apr 26 17:29:29 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42296->web.edu:80)
Apr 26 17:29:29 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:42295->web.edu:80)
Apr 26 17:29:29 port 25749 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:25749)
Apr 26 17:29:29 http connection closed from PortScan@paradise.net.nz [203.96.152.186]

(203.96.152.186:42236->web.edu:80)

--SNIP –

Apr 26 17:54:33 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7658->web.edu:80)
Apr 26 17:54:33 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7556->web.edu:80)
Apr 26 17:54:35 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7658->web.edu:80)
Apr 26 17:54:35 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7658->web.edu:80)
Apr 26 17:54:37 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7717->web.edu:80)
Apr 26 17:54:37 port 26732 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26732)
Apr 26 17:54:39 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7717->web.edu:80)
Apr 26 17:54:39 port 26732 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26732)
Apr 26 17:54:39 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7658->web.edu:80)
Apr 26 17:54:39 port 26732 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26732)
Apr 26 17:54:39 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7717->web.edu:80)
Apr 26 17:54:39 port 26733 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26733)
Apr 26 17:54:39 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:7717->web.edu:80)
Apr 26 17:54:39 port 26733 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26733)
Apr 26 17:54:39 port 26734 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26734)
Apr 26 17:54:39 port 26735 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:26735)

(7B-2) ippl log on web.edu from PARADISE-NZ-WEBBINF
May 4 22:41:18 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:65224->web.edu:80)
May 4 22:41:20 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:65250->web.edu:80)
May 4 22:41:20 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:65224->web.edu:80)
May 4 22:41:20 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:65250->web.edu:80)
May 4 22:41:20 port 28397 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:28397)
May 4 22:41:20 port 28398 connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:113->web.edu:28398)

(7B-3) ippl log on web.edu from PARADISE-NZ-WEBBINF
May 7 03:07:31 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:46636->web.edu:80)
May 7 03:07:31 http connection closed from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:46636->web.edu:80)
May 7 03:07:32 http connection attempt from PortScan@paradise.net.nz [203.96.152.186]
(203.96.152.186:46689->web.edu:80)

May 7 03:07:32 http connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:46689->web.edu:80)
May 7 03:07:32 port 27193 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:27193)
May 7 03:07:32 port 27194 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:27194)

(7B-4) ippl log on web.edu from PARADISE-NZ-WEBBINF
May 18 04:17:47 http connection attempt from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:39748->web.edu:80)
May 18 04:17:47 http connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:39748->web.edu:80)
May 18 04:17:47 port 7112 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:7112)
May 18 04:17:48 port 7112 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:7112)
May 18 04:17:58 http connection attempt from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:40401->web.edu:80)
May 18 04:17:58 port 7113 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:7113)
May 18 04:18:01 http connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:40401->web.edu:80)
May 18 04:18:11 http connection attempt from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:40799->web.edu:80)
May 18 04:18:11 port 7114 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:7114)
May 18 04:18:11 http connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:40799->web.edu:80)
May 18 04:18:12 port 7114 connection closed from PortScan@paradise.net.nz [203.96.152.186] (203.96.152.186:113->web.edu:7114)

(7B-5) ippl log on web.edu from PARADISE-NZ-WEBBINF
May 22 07:45:13 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1645-> web.edu:80)
May 22 07:45:18 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1646-> web.edu:80)
May 22 07:45:22 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1647-> web.edu:80)
May 22 07:45:23 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1648-> web.edu:80)
May 22 07:45:27 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1646-> web.edu:80)
May 22 07:45:30 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1647-> web.edu:80)
May 22 07:45:31 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1648-> web.edu:80)
May 22 07:45:31 port 10993 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10993)
May 22 07:45:31 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1645-> web.edu:80)
May 22 07:45:36 port 10995 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10995)
May 22 07:45:36 port 10996 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10996)
May 22 07:45:36 port 10995 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10995)
May 22 07:45:36 port 10997 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10997)

May 22 07:45:36 port 10998 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10998)
May 22 07:45:36 port 10999 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10999)
May 22 07:45:36 port 10998 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10998)
May 22 07:45:36 port 10999 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:10999)
May 22 07:45:54 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1649-> web.edu:80)

--SNIP—

May 22 08:00:04 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1674-> web.edu:80)
May 22 08:00:12 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1676-> web.edu:80)
May 22 08:00:17 http connection attempt from PortScan.fr[130.120.81.42] (130.120.81.42:1679-> web.edu:80)
May 22 08:00:22 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1677-> web.edu:80)
May 22 08:00:23 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1680-> web.edu:80)
May 22 08:00:23 port 11186 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:11186)
May 22 08:00:37 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1678-> web.edu:80)
May 22 08:00:38 http connection attempt from PortScan.fr [130.120.81.42] (130.120.81.42:1681-> web.edu:80)
May 22 08:00:38 port 11187 connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:113-> web.edu:11187)
May 22 08:02:01 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1679-> web.edu:80)
May 22 08:02:06 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1680-> web.edu:80)
May 22 08:02:20 http connection closed from PortScan.fr [130.120.81.42] (130.120.81.42:1681-> web.edu:80)

(7C-1) ippl log on web.edu
May 15 20:54:11 ftp connection attempt from Scan.http [24.31.228.189] (24.31.228.189:1364-> web.edu:21)
May 15 20:54:11 port 30914 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:1365-> web.edu:30914)
May 15 20:54:11 port 30914 connection closed from Scan.http [24.31.228.189] (24.31.228.189:1365-> web.edu:30914)
May 15 20:54:23 ftp connection closed from Scan.http [24.31.228.189] (24.31.228.189:1364-> web.edu:21)

(7C-2) ippl log on web.edu
May 16 00:17:42 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2663-> web.edu:80)
May 16 00:17:43 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2664-> web.edu:80)
May 16 00:21:59 ftp connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2692-> web.edu:21)

May 16 00:22:00 port 2065 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2693-> web.edu:2065)
May 16 00:22:00 port 2065 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2693-> web.edu:2065)
May 16 00:22:36 port 2067 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2697-> web.edu:2067)
May 16 00:22:36 port 2067 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2697-> web.edu:2067)
May 16 00:22:36 port 2069 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2699-> web.edu:2069)
May 16 00:22:37 port 2069 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2699-> web.edu:2069)
May 16 00:22:49 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2701-> web.edu:80)
May 16 00:23:12 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2704-> web.edu:80)
May 16 00:24:28 port 2073 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2712-> web.edu:2073)
May 16 00:24:29 port 2073 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2712-> web.edu:2073)
May 16 00:24:29 port 2075 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2713-> web.edu:2075)
May 16 00:24:29 port 2075 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2713-> web.edu:2075)
May 16 00:26:26 port 2077 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2726-> web.edu:2077)
May 16 00:26:26 port 2077 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2726-> web.edu:2077)
May 16 00:26:27 port 2079 connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2727-> web.edu:2079)
May 16 00:26:27 port 2079 connection closed from Scan.http [24.31.228.189] (24.31.228.189:2727-> web.edu:2079)
May 16 00:26:41 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2729-> web.edu:80)
May 16 00:27:36 ftp connection closed from Scan.http [24.31.228.189] (24.31.228.189:2692-> web.edu:21)
May 16 00:29:25 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2752-> web.edu:80)
May 16 00:29:25 http connection closed from Scan.http [24.31.228.189] (24.31.228.189:2752-> web.edu:80)
May 16 00:31:22 http connection attempt from Scan.http [24.31.228.189] (24.31.228.189:2767-> web.edu:80)

(7C-3) Syslogd on web.edu
May 15 20:54:06 www1 in.ftpd[9055]: connect from 24.31.228.189
May 15 20:54:07 www1 ftpd[9055]: FTP LOGIN FROM Scan.http [24.31.228.189], ftp-user
May 16 00:21:59 www1 in.ftpd[470]: connect from 24.31.228.189
May 16 00:21:59 www1 ftpd[470]: FTP LOGIN FROM Scan.http [24.31.228.189], ftp-user

Source of Traces

Detect 7A	ippl log on Tutorial Education Network web server (web.edu)
Detect 7B1	ippl log on Tutorial Education Network web server (web.edu)
Detect 7B2	ippl log on Tutorial Education Network web server (web.edu)
Detect 7B3	ippl log on Tutorial Education Network web server (web.edu)
Detect 7B4	ippl log on Tutorial Education Network web server (web.edu)
Detect 7B5	ippl log on Tutorial Education Network web server (web.edu)
Detect 7C-1	ippl log on Tutorial Education Network web server (web.edu)

Detect 7C-2	Data collected from Tutorial Education Network web server (web.edu
Detect 7C-3	Syslogd log on web.edu

Detects were generated by

Detect 7A	Unix Port Sentry. Detailed information of product is located at http://www.psionic.com/abacus/portsentry/
Detect 7B	Data collected using Unix ippl logging facility information at (http://pltplp.net/ippl/) Grep was use on IP address.
Detect 7C1	Data collected using Unix ippl logging facility information at (http://pltplp.net/ippl/)
Detect 7C2	Data collected using Unix ippl logging facility information at (http://pltplp.net/ippl/)
Detect 7C3	Data collected from Unix Syslogd. Log checker mails syslogd event back to admin

Probability that source address was spoofed

Detect 7A	This was probably not a spoofed address.
Detect 7B	Scan covered my portion of a Class C network. Hit two machines in two minutes, This was probably not a spoofed address.
Detect 7C1-3	This was probably not a spoofed address. Appears to be a user updating their web site. Ftp connection recorded in log file by syslogd. No Port 113 noticed either.

Description of Attack

Quote attributed to (http://www.blueneptune.com/~yingda/socks/SOCKS4.protocol). Access control can be applied at the beginning of each TCP session;thereafter the server simply relays the data between the client and the application server, incurring minimum processing overhead. Since SOCKS never has to know anything about the application protocol, it should also be easy for it to accommodate applications which use encryption to protect their traffic from nosey snoopers.

Detect 7A-B	Something strange here. Port 113 is involved with connection when a port is closed. Why is this so? No record of port 113 opening any ports. I need better logging tools. Smell like crafted IP packets.
Detect 7C1	This is an example of user updating their Web page using ftp. Normal network behavior.
Detect 7C2	Same user checking web page again. No port 113 noticed.
Detect 7C3	This is an example of user updating their Web page using ftp. Normal network behavior. Same port scanning behavior exhibited in 7A&B but no Port 113 noticed.

Attack Method

Detect 7A1-7B5	Users are appearing to requesting opening of a http port than they are next show closing different port sequences. They appear to then start communication off port 113 from their machine.
Detect 7C1-7C3	No Attack, user updating web page using ftp. Trace located to try and determine what would cause so many http connection request an new port show closing.

Correlation

Detect 7A-B	I believe these two IP address came from SANS GIAC reports. Bad documentation on my part, so I can't verify it now, the port 113 traffic, scary. I really need more logging capability.
Detect 7C	None.

Evidence of active targeting

Detect 7A-B	The use of port 113 makes me wonder if someone knows more than me about the services available from my web server. It appears to be some type of socks available. The port sequence exchange is to regular with the involvement of Port 113.

Detect 7C	Detect from search to looking what I considered valid traffic. I wanted to see if the Port 113 was truly required so much, or to help determine if it was being abused.

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 7A	(5 + 5) – (3 + 1) = 6
Detect 7B	(5 + 5) – (3 + 1) = 6
Detect 7C	(5 + 5) – (3 + 1) = 6

Defensive Recommendation

Detect 7A-B	Psionic tools (http://www.psionic.com/abacus/portsentry/) really are great!!! It looks like time to remove some services from machine and increase logging capabilities.
Detect 7C	None required, appears to be normal client\server relation. No suspicious port use displayed.

Multiple Choice Test Question

Detect 7A	The port switch behavior displayed with the use of Port 113 is an example of what service..
Detect 7B	The FTP connection in trace C works on what port

Choices

A.	Socks
B	113
C	21
D	DNS

Answers 7A-A 7B-C

Detect #8 (DNS Probe)
Taken from the following article http://advice.networkice.com/advice/Intrusions/2003011/?port=53
Scan. A hacker may be scanning your system to see if the DNS service is available on your system. Sometimes this is done in preparation for a future attack, or sometimes it is done to see if your system might be susceptible to attack.

(8A) ippl log on web.edu from SE-KOPINGSKABEL-TV
May 20 19:12:43 domain connection attempt from unknown@pc184.net20.ktv.koping.se [195.163.20.184] (195.163.20.184:65535->web.edu:53)

(8B) ippl log on web.edu from JPNIC-NET-JP
Jun 2 21:47:37 port 53 connection attempt from unknown@dns1.udc-c.dion.ne.jp [210.196.222.18] (210.196.222.18:53->web.edu:53)
Jun 2 21:47:37 port 17154 connection closed from dns1.udc-c.dion.ne.jp [210.196.222.18] (210.196.222.18:113->web.edu:17154)

Source of Traces

Detect 8A	Data collected from Education web server (web.edu) that is running Linux
Detect 8B	Data collected from Education web server (web.edu) that is running Linux

Detects were generated by

Detect 8A-B	Data collected using Unix ippl logging facility http://pltplp.net/ippl/ Grep command used on port IP address.

Probability that source address was spoofed

Detect 8A-B	This was probably not a spoofed address. Someone looking for DNS or some other type of service.

Description of Attack

Detect 8A	From correlations given on previous GIAC reports, it appear to be an automated scan searching through the Internet for DNS. Tool appears to have crafted packets due to the common occurrence of a source port of 65535.
Detect 8B	From correlation on previous GIAC report it appears to be a tool of some type. It appears to also exhibit similar port behavior to Detect 1C. Notice the strange port open port closed patteren from a port never logged as open. Once again we see Port 113 at work. It appears this port is involved in a lot of strange activity on this server and other GIAC reports.

Correlation

Detect 8A	Detect attributed to Lisa Yeos for the source port match in http://www.sans.org/y2k/052100.htm. Roger Lutz, GCIA in http://www.sans.org/y2k/052500.htm for the IP address.
Detect 8B	Detect attributed to Ostroot, Judith M from http://www.sans.org/y2k/060300.htm.

Evidence of active targeting

Detect 8A	IP address was seen in multiple GIAC reports looking for DNS.
Detect 8B	IP address from same network was noticed in other GIAC report with SYN-FYN settings

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity

Detect 8A	(5 + 3) – (3 + 2) = 3
Detect 8B	(5 + 3) – (3 + 2) = 3

Defensive Recommendation

Detect 8A-B Since this machines does not run DNS, Port Sentry would have been nice to have stop probe and drop the offending address into a routing black hole.

Multiple Choice Test Question

Detect 8

Match Question with Choices

8. Port 53 allows for running what services?

Choices

A DNS
B Pop3
C Linuxconf
D Sunrpc

Answers 8A

Detect #9 (FTP Attempt)

(9) ippl log on web.edu from Chunghwa Telecom Co., Ltd. Data communication
May 9 22:15:14 ftp connection attempt from unknown@203.66.211.246 (203.66.211.246:3086-> web.edu:21)
May 9 22:15:14 ftp connection closed from [203.66.211.246] (203.66.211.246:3086->web.edu:21)

Source of Traces
Detect 9 Data collected from Education web server (web.edu) that is running Linux

Detects were generated by
Detect 9 Data collected using Unix ippl logging facility http://pltplp.net/ippl/ Grep command used on port IP address..

Probability that source address was spoofed
Detect 9 This was not a spoofed address. Someone is actively mining the Internet looking for ftp access

Description of Attack
Detect 9 Scanning tool that attempts to access ftp services. This machine is running ftp, data mining was successful at this site..

Correlation
Detect 9 This detect is originally attributed to Laurie @ edu (http://www.sans.org/y2k/051900.htm) Paul and Josh noticed them too in (http://www.sans.org/y2k/052400.htm) Pierre Lamy saw the same network, but a different IP address in http://www.sans.org/y2k/052400-1300.htm) looking for linuxconf.

Evidence of active targeting
Detect 9 User was only seen once at this site looking for just the ftp services. User seen in multiple GIAC reports looking for ftp services.

Severity

Defensive Recommendation
Detect 9 FTP services required for users running web pages. SSH reduces the risk of ftp, but requires re-training users base. Port Sentry would have blocked nicely, but FTP is a valid service for this computer.

Multiple Choice Test Question
Detect 9

Match Question with Choices
(Critical + Lethal) – (System + Net Countermeasures) = Severity
Detect 9 (5 + 5) – (3 + 2) = 5

Choices
A Wide
B Narrow
C Wide & Narrow
D None of the above
Answers 9 C

Detect #10 (Nebious Traffice)
Tcp requires a three-way handskake betwent the client and server before a connection can be established and data transferred. (Slide 2-14 SANS San Jose 2.1 TCP/IP for intrusion Detection and Perimeter Defense.)

(10A) tcpdump from internal network between Microsoft 95 client and Domain Controllerippl log
:10:30:21.834566 Student-c.edu.1433 > server.edu.139: S 508517653:508517653(0) win 8192 <mss 1460> (DF)
:10:30:21.834566 server.edu.139 > Student-c.edu.1433: S 560412124:560412124(0) ack 508517654 win 8760 <mss 1460> (DF)
:10:30:21.834566 Student-c.edu.1433 > server.edu.139: . ack 1 win 8760 (DF)
:10:30:21.834566 Student-c.edu.1433 > server.edu.139: P 1:73(72) ack 1 win 8760 (DF)
:10:30:21.834566 server.edu.139 > Student-c.edu.1433: P 1:5(4) ack 73 win 8688 (DF)
:10:30:21.854566 Student-c.edu.1433 > server.edu.139: P 73:231(158) ack 5 win 8756 (DF)
:10:30:21.874566 server.edu.139 > Student-c.edu.1433: P 5:104(99) ack 231 win 8530 (DF)
:10:30:21.884566 Student-c.edu.1433 > server.edu.139: P 231:393(162) ack 104 win 8657 (DF)
:10:30:21.974566 server.edu.139 > Student-c.edu.1433: P 104:206(102) ack 393 win 8368 (DF)
:10:30:21.984566 Student-c.edu.1433 > server.edu.139: P 393:542(149) ack 206 win 8555 (DF)
:10:30:22.024566 server.edu.139 > Student-c.edu.1433: P 206:582(376) ack 542 win 8219 (DF)
:10:30:22.074566 Student-c.edu.1433 > server.edu.139: P 542:691(149) ack 582 win 8179 (DF)
:10:30:22.114566 server.edu.139 > Student-c.edu.1433: P 582:958(376) ack 691 win 8070 (DF)
:10:30:22.304566 Student-c.edu.1433 > server.edu.139: . ack 958 win 7803 (DF)
:10:30:23.444566 Student-c.edu.1433 > server.edu.139: P 691:730(39) ack 958 win 7803 (DF)
:10:30:23.454566 server.edu.139 > Student-c.edu.1433: P 958:997(39) ack 730 win 8031 (DF)
:10:30:23.454566 Student-c.edu.1433 > server.edu.139: F 730:730(0) ack 997 win 7764 (DF)
:10:30:23.454566 server.edu.139 > Student-c.edu.1433: F 997:997(0) ack 731 win 8031 (DF)
:10:30:23.454566 Student-c.edu.1433 > server.edu.139: . ack 998 win 7764 (DF)

Source of Traces
Detect 10 Data collected from Education name server (name.edu) that is running Linux

Detects were generated by
Detect 10 Data collected using Unix tcpdump. Filtering performed by using grep command from log. Trace perform to provide feedback on what a good exchange should like. Starting have doubts about it after seeing so many port 113 connections in other area of data collected.

Probability that source address was spoofed
Detect 10 This was not a spoofed address. Two machines on same network passing Microsoft crap.

Description of Attack
Detect 10 Normal package exchange of chatty Microsoft netbios.

Correlation
Detect 10 Watched using tcpdump information.

Evidence of active targeting
Detect 10 None

Severity

(Critical + Lethal) – (System + Net Countermeasures) = Severity
Detect 10A (1 + 1) – (3 + 2) = -3

Defensive Recommendation
Detect 8A-B None required, example of clean 3-way handshake.and passing of packets.

Multiple Choice Test Question
Detect 10

Match Question with Choices
10-1 This connection termination is an _____ example termination
10-2 What is the initial ephemeral port number.

Choices

A	Abrupt
B	Graceful
C	1433
D	139

Answers 10-1 B 10-2 C