Global Information Assurance Certification Paper

*** Northcutt, very nice example of the I&W analysis process, got his own detects, detect 8 is probably load balancing. 94 ***

GIAC Certified Intrusion Analyst Practical Detects Assignment

Student Name: Eric Brock

Date: April 4, 2000

Notes About Detects:
All of these detects were taken from Firewall-1 logs. Our firewall sits between our DMZ servers and the Internet. All of the packets logged in these detects were dropped by the firewall, which is why there is no traffic seen in the opposite direction. Part of our intrusion detection strategy consists of loading our firewall logs into a database and querying the database for events of interest. This is what is seen here, which explains why these detects will not look like a typical Firewall-1 log.

About Our Network:
We have a class C address block. All of our addresses (seen in the DestIP column) have been replaced with 10.10.1.x addresses. The names of our servers that appear in these traces have been changed: our DNS server is seen as “dns.our.dmz”, our proxy server is seen as “proxy.our.dmz”, and our mail server is seen as “mail.our.dmz”. SourceIP addresses have not been changed, nor has any other information. All of these servers have an interface with a valid Internet address.

Detect # 1

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
15670	10Aug1999	22:39:06	200-211-160-28-as.acessonet.com.br	60000	10.10.1.1	2140	udp	len 30
15671	10Aug1999	22:39:06	200-211-160-28-as.acessonet.com.br	60000	10.10.1.2	2140	udp	len 30
15672	10Aug1999	22:39:06	200-211-160-28-as.acessonet.com.br	60000	10.10.1.3	2140	udp	len 30
15673	10Aug1999	22:39:06	200-211-160-28-as.acessonet.com.br	60000	10.10.1.4	2140	udp	len 30
…	…	…	…	…	…	…	…	…
15921	10Aug1999	22:39:27	200-211-160-28-as.acessonet.com.br	60000	10.10.1.252	2140	udp	len 30
15922	10Aug1999	22:39:27	200-211-160-28-as.acessonet.com.br	60000	10.10.1.253	2140	udp	len 30
15923	10Aug1999	22:39:27	200-211-160-28-as.acessonet.com.br	60000	10.10.1.254	2140	udp	len 30
15924	10Aug1999	22:39:27	200-211-160-28-as.acessonet.com.br	60000	10.10.1.255	2140	udp	len 30

Existence: Someone claiming to be 200-211-160-28-as.acessonet.com.br (Brazil) is visiting us.

History: There is no other history of this host or network visiting our network.

Techniques: The source port is constant (60000). The packets are coming fast (the entire class C scan is completed in 21 seconds). One packet is being sent to each address on our subnet in sequential order.

Intent: The intent is to find a server on our subnet that will respond on UDP port 2140.

Targeting: Our class C subnet is being targeted, but no specific machines are being targeted.

Analysis: The constant source port of 60000 gives this scan a definite fingerprint. That, combined with the speed, indicates that a scripted tool is being used. This is a scan looking for a host listening on UDP port 2140. Because the DeepThroat trojan is known to use this port, it is safe to conclude that this is a trojan scan for the DeepThroat trojan.

Severity:

Component	Score	Comments
Criticality	3	No specific machines are being targeted
Lethality	5	DeepThroat is a very lethal vulnerability
System Countermeasures	4	All operating systems are running the latest patches.
Network Countermeasures	4	Firewall blocks all packets to port 2140
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 2

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
661530	21Feb2000	9:09:24	195.243.30.140	4858	10.10.1.1	ftp	tcp	len 60
661531	21Feb2000	9:09:24	195.243.30.140	4857	10.10.1.0	ftp	tcp	len 60
661532	21Feb2000	9:09:24	195.243.30.140	4860	10.10.1.3	ftp	tcp	len 60
661533	21Feb2000	9:09:24	195.243.30.140	4859	10.10.1.2	ftp	tcp	len 60
…	…	…	…	…	…	…	…	…
661632	21Feb2000	9:09:25	195.243.30.140	1144	10.10.1.252	ftp	tcp	len 60
661633	21Feb2000	9:09:25	195.243.30.140	1145	10.10.1.253	ftp	tcp	len 60
661634	21Feb2000	9:09:25	195.243.30.140	1146	10.10.1.254	ftp	tcp	len 60

Existence: Someone claiming to be IP address 195.243.30.140 is visiting us.

History: There is no history of this address visiting our network.

Techniques: The visitor is sending one FTP packet to each address in our subnet. They are being sent extremely fast.

Intent: The visitor is attempting find hosts on our network that will respond on the FTP port.

Targeting: Our entire network is being targeted, but no specific servers.

Analysis: This visitor is performing a scan of our network looking for FTP servers. The visitor could be planning a denial of service against an FTP server, or he could be looking for an anonymous FTP server to see what he can download from it, or to see what he can upload to it.

Severity:

Component	Score	Comments
Criticality	3	No specific servers are targeted.
Lethality	4	There are many known FTP vulnerabilities
System Countermeasures	2	All operating systems are running the latest patches, but some are listening on the FTP port.
Network Countermeasures	4	Firewall blocks all incoming FTP.
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 3

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
3686	3Aug1999	18:48:56	195.34.20.139	31790	10.10.1.1	31789	udp	len 29
3693	3Aug1999	18:48:56	195.34.20.139	31790	10.10.1.2	31789	udp	len 29
3694	3Aug1999	18:48:56	195.34.20.139	31790	10.10.1.3	31789	udp	len 29
…	…	…	…	…	…	…	…	…
3928	3Aug1999	18:49:05	195.34.20.139	31790	10.10.1.254	31789	udp	len 29
3930	3Aug1999	18:49:05	195.34.20.139	31790	10.10.1.253	31789	udp	len 29
8005	6Aug1999	3:18:45	dialup-147.basri.net	31790	10.10.1.255	31789	udp	len 29
9887	7Aug1999	3:44:33	193.188.121.198	31790	10.10.1.1	31789	udp	len 29
9888	7Aug1999	3:44:33	193.188.121.198	31790	10.10.1.2	31789	udp	len 29
9889	7Aug1999	3:44:33	193.188.121.198	31790	10.10.1.3	31789	udp	len 29
…	…	…	…	…	…	…	…	…
10058	7Aug1999	3:44:34	193.188.121.198	31790	10.10.1.253	31789	udp	len 29
10059	7Aug1999	3:44:34	193.188.121.198	31790	10.10.1.254	31789	udp	len 29
10060	7Aug1999	3:44:34	193.188.121.198	31790	10.10.1.255	31789	udp	len 29
36564	19Aug1999	21:18:16	208.31.76.52	31790	10.10.1.1	31789	udp	len 29
36565	19Aug1999	21:18:17	208.31.76.52	31790	10.10.1.3	31789	udp	len 29
…	…	…	…	…	…	…	…	…
36691	19Aug1999	21:18:18	208.31.76.52	31790	10.10.1.253	31789	udp	len 29
36692	19Aug1999	21:18:18	208.31.76.52	31790	10.10.1.255	31789	udp	len 29
67793	30Aug1999	12:50:15	212.217.13.204	31790	10.10.1.1	31789	udp	len 29
67794	30Aug1999	12:50:15	212.217.13.204	31790	10.10.1.2	31789	udp	len 29
67795	30Aug1999	12:50:15	212.217.13.204	31790	10.10.1.3	31789	udp	len 29
…	…	…	…	…	…	…	…	…
67901	30Aug1999	12:50:16	212.217.13.204	31790	10.10.1.254	31789	udp	len 29

Existence: Multiple IP addresses are visiting us in these traces.

History: There is no history of any of these addresses visiting our network. All of the detects were within the same month (August 1999)

Techniques: The visitors are sending packets to UDP port 31790, and always with a source port of 31789. Each visitor scans our entire class C network in this manner. The packets are sent very fast.

Intent: The visitor is attempting find hosts on our network that will respond on UDP port 31790.

Targeting: Our entire network is being targeted, but no specific servers.

Analysis: The fast nature of these scans and the fixed source port indicate a script is being used that crafts packets. UDP port 31790 is the port used by the Windows Hack-a-Tack trojan. All of these traces are scans to find instances of this trojan.

Severity:

Component	Score	Comments
Criticality	3	No specific servers are targeted.
Lethality	5	Windows Hack-a-Tack is a very lethal vulnerability.
System Countermeasures	4	All operating systems are running the latest patches, and none are listening on UDP 31790.
Network Countermeasures	4	Firewall blocks UDP port 31790.
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 4

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
74523	1Sep1999	15:46:05	dialup98.gent.skynet.be	1107	10.10.1.1	31337	udp	len 46
74524	1Sep1999	15:46:05	dialup98.gent.skynet.be	1107	10.10.1.2	31337	udp	len 46
74525	1Sep1999	15:46:05	dialup98.gent.skynet.be	1107	10.10.1.3	31337	udp	len 46
…	…	…	…	…	…	…	…	…
74775	1Sep1999	15:46:19	dialup98.gent.skynet.be	1107	10.10.1.253	31337	udp	len 46
74776	1Sep1999	15:46:19	dialup98.gent.skynet.be	1107	10.10.1.254	31337	udp	len 46
74777	1Sep1999	15:46:19	dialup98.gent.skynet.be	1107	10.10.1.255	31337	udp	len 46

Existence: Someone claiming to be dialup98.gent.skynet.be (Belgium) is visiting us.

History: There is no other history of this host or network visiting our network.

Techniques: The source port is constant (1107). One packet is being sent to each address in our subnet in a sequential manner. The packet are coming in fast.

Intent: The intent is to find a server on our subnet that will respond on UDP port 31337.

Targeting: Our class C subnet is being targeted, but no specific machines are being targeted.

Analysis: The constant source port of 1107 gives this scan a definite fingerprint. The visitor seems to be using a script that crafts packets and sequentially scans an entire class C subnet. This is a scan looking for a host listening on UDP port 31337. Because the Back Orifice trojan is known to use this port, it is safe to conclude that this is a trojan scan for Back Orifice.

Severity:

Component	Score	Comments
Criticality	3	No specific machines are being targeted
Lethality	5	Back Orifice is a very lethal vulnerability
System Countermeasures	4	All operating systems are running the latest patches.
Network Countermeasures	4	Firewall blocks all packets to port 31337
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 5

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
703375	6Mar2000	8:13:59	tt.deltamax.com	telnet	10.10.1.1	telnet	tcp	len 40
703376	6Mar2000	8:13:59	tt.deltamax.com	telnet	10.10.1.2	telnet	tcp	len 40
703377	6Mar2000	8:13:59	tt.deltamax.com	telnet	10.10.1.3	telnet	tcp	len 40
703378	6Mar2000	8:13:59	tt.deltamax.com	http	10.10.1.1	http	tcp	len 40
703379	6Mar2000	8:13:59	tt.deltamax.com	smtp	10.10.1.2	smtp	tcp	len 40
703380	6Mar2000	8:13:59	tt.deltamax.com	pop3	10.10.1.4	pop3	tcp	len 40
703381	6Mar2000	8:13:59	tt.deltamax.com	http	10.10.1.4	http	tcp	len 40
703382	6Mar2000	8:14:03	tt.deltamax.com	telnet	10.10.1.5	telnet	tcp	len 40
703383	6Mar2000	8:14:03	tt.deltamax.com	telnet	10.10.1.6	telnet	tcp	len 40
703384	6Mar2000	8:14:03	tt.deltamax.com	telnet	10.10.1.7	telnet	tcp	len 40
703411	6Mar2000	8:14:03	tt.deltamax.com	imap	10.10.1.5	imap	tcp	len 40
703411	6Mar2000	8:14:03	tt.deltamax.com	imap	10.10.1.5	imap	tcp	len 40
703412	6Mar2000	8:14:03	tt.deltamax.com	imap	10.10.1.7	imap	tcp	len 40
703413	6Mar2000	8:14:03	tt.deltamax.com	imap	10.10.1.8	imap	tcp	len 40
…	…	…	…	…	…	…	…	…
704210	6Mar2000	8:14:36	tt.deltamax.com	pop3	10.10.1.253	pop3	tcp	len 40
704211	6Mar2000	8:14:36	tt.deltamax.com	http	10.10.1.252	http	tcp	len 40
704212	6Mar2000	8:14:36	tt.deltamax.com	http	10.10.1.253	http	tcp	len 40
704213	6Mar2000	8:14:36	tt.deltamax.com	telnet	10.10.1.255	telnet	tcp	len 40
704214	6Mar2000	8:14:36	tt.deltamax.com	smtp	10.10.1.254	smtp	tcp	len 40
704215	6Mar2000	8:14:36	tt.deltamax.com	smtp	10.10.1.255	smtp	tcp	len 40
704216	6Mar2000	8:14:36	tt.deltamax.com	imap	10.10.1.254	imap	tcp	len 40
704217	6Mar2000	8:14:36	tt.deltamax.com	imap	10.10.1.255	imap	tcp	len 40
704218	6Mar2000	8:14:36	tt.deltamax.com	pop3	10.10.1.254	pop3	tcp	len 40
704219	6Mar2000	8:14:36	tt.deltamax.com	pop3	10.10.1.255	pop3	tcp	len 40
704220	6Mar2000	8:14:36	tt.deltamax.com	http	10.10.1.254	http	tcp	len 40
704221	6Mar2000	8:14:36	tt.deltamax.com	http	10.10.1.255	http	tcp	len 40

Existence: Someone claiming to be tt.deltamax.com is visiting us.

History: There is no history of this visitor visiting our network.

Techniques: The visitor is sending packets to our entire subnet using four different destination ports: HTTP, POP3, TELNET, and IMAP. One packet of each of the four types is being sent to each address on our class C subnet. They are being sent very fast, up to 75 packets per second. The source port is always the same as the destination port.

Intent: The visitor is attempting find hosts on our network that will respond to any of the four ports listed above.

Targeting: Our entire network is being targeted, but no specific servers.

Analysis: The source port always being equal to the destination port indicates that the packets are crafted, and combined with the speed of the scan it can be concluded that a script is being used.

This is a hybrid of a host scan and port scan. The visitor would like to find the servers on our network that will respond to a connection attempt on HTTP, POP3, TELNET, or IMAP. All of these ports have known vulnerabilities.

Severity:

Component	Score	Comments
Criticality	3	No specific servers are targeted.
Lethality	5	All of the ports have known vulnerabilities that could prove lethal.
System Countermeasures	2	All operating systems are running the latest patches, but some are listening on these ports.
Network Countermeasures	4	Firewall blocks all HTTP, POP3, TELNET, and IMAP packets inbound to servers
Severity Score	2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 6

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
122954	24Sep1999	0:16:55	01-042.032.popsite.net		10.10.1.255		icmp	icmp-type 8 icmp-code 0
122955	24Sep1999	0:16:55	01-042.032.popsite.net		10.10.1.0		icmp	icmp-type 8 icmp-code 0
124567	24Sep1999	11:24:04	01-062.032.popsite.net		10.10.1.0		icmp	icmp-type 8 icmp-code 0
124568	24Sep1999	11:24:04	01-062.032.popsite.net		10.10.1.255		icmp	icmp-type 8 icmp-code 0

Existence: Someone claiming to be 01-042.032.popsite.net is visiting us.

History: The visitor came just after midnight on 9/24/99, and again 11 hours later. There is no other history of this host or network visiting our network.

Techniques: The visitor came at two different times on the same day. Both times, an ICMP type 8 packet (echo request) is sent to the .255 and .0 address of our class C subnet.

Intent: The visitor is attempting to discover any hosts that will respond with an echo reply.

Targeting: Our class C subnet is being targeted, but no specific machines are being targeted.

Analysis: This is an attempt to map our network using ICMP echo request broadcast packets. Any host that responds will reveal its existence to the visitor.

Also, the visitor can learn something about the systems that might respond based on which packet they respond to (.0 or .255). Most TCP/IP stacks treat a .255 in the fourth octet as a broadcast address. TCP/IP stacks based on the UNIX BSD operating system will respond to a .0 as being the broadcast address.

In addition, the visitor might find a router that would return a host unreachable message for the servers or subnets that do not exist, which the visitor could use to do an inverse mapping of our network.

Severity:

Component	Score	Comments
Criticality	3	No specific machines are being targeted
Lethality	3	It is unknown how the visitor would use any information gathered in this mapping attempt.
System Countermeasures	2	All operating systems are running the latest patches, but they will all respond to an ICMP echo request.
Network Countermeasures	4	Firewall blocks all ICMP packets
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 7

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
726624	13Mar2000	7:10:14	155.253.16.49	44421	mail.our.dmz	33486	udp	len 40
726625	13Mar2000	7:10:17	155.253.16.49	44421	mail.our.dmz	33487	udp	len 40
726627	13Mar2000	7:10:20	155.253.16.49	44421	mail.our.dmz	33488	udp	len 40
726628	13Mar2000	7:10:25	155.253.16.49	44421	mail.our.dmz	33489	udp	len 40
726629	13Mar2000	7:10:28	155.253.16.49	44421	mail.our.dmz	33490	udp	len 40
726630	13Mar2000	7:10:31	155.253.16.49	44421	mail.our.dmz	33491	udp	len 40
726631	13Mar2000	7:10:34	155.253.16.49	44421	mail.our.dmz	33492	udp	len 40
726632	13Mar2000	7:10:37	155.253.16.49	44421	mail.our.dmz	33493	udp	len 40
726633	13Mar2000	7:10:40	155.253.16.49	44421	mail.our.dmz	33494	udp	len 40
…	…	…	…	…	…	…	…	…
726648	13Mar2000	7:11:25	155.253.16.49	44421	mail.our.dmz	33509	udp	len 40
726649	13Mar2000	7:11:28	155.253.16.49	44421	mail.our.dmz	33510	udp	len 40
726650	13Mar2000	7:11:31	155.253.16.49	44421	mail.our.dmz	33511	udp	len 40
726651	13Mar2000	7:11:34	155.253.16.49	44421	mail.our.dmz	33512	udp	len 40
726652	13Mar2000	7:11:37	155.253.16.49	44421	mail.our.dmz	33513	udp	len 40
726653	13Mar2000	7:11:40	155.253.16.49	44421	mail.our.dmz	33514	udp	len 40
726654	13Mar2000	7:11:45	155.253.16.49	44421	mail.our.dmz	33515	udp	len 40
726655	13Mar2000	7:11:48	155.253.16.49	44421	mail.our.dmz	33516	udp	len 40
726656	13Mar2000	7:11:51	155.253.16.49	44421	mail.our.dmz	33517	udp	len 40
726657	13Mar2000	7:11:54	155.253.16.49	44421	mail.our.dmz	33518	udp	len 40

Existence: Someone claiming to be 155.253.16.49 is visiting us.

History: There is no history of this address visiting our network.

Techniques: The visitor is sending a UDP packet to our mail server on some of the high UDP ports. These packets are coming like clockwork every 3 seconds. The ports range from 33486 to 33518. The source port is always 44421.

Intent: The visitor is attempting find out what UDP ports between 33486 and 33518 are open on our mail server.

Targeting: Our mail server is the target of this scan.

Analysis: Because the packets are coming in at a constant rate, it is likely a program is being used. The program being used is traceroute, which uses UDP ports 33434 through 33523. While the constant source port of 44421 initially looks suspicious, it is consistent with how traceroute operates. We can also determine that this is not a Microsoft operating system, as Microsoft operating systems use ICMP exclusively for traceroute.

This visitor is attempting to map out the routing structure of our network. It would not be surprising to see other traceroute attempts to our mail server at different times during the day. By doing this, the visitor could determine how many routes there are in to our network, and thus locate single points of failure for a future denial of service attack.

Severity:

Component	Score	Comments
Criticality	5	Our mail server is being directly targeted.
Lethality	4	A denial of service attack on our network would be lethal.
System Countermeasures	4	All operating systems are running the latest patches, and none are listening on any of the UDP ports in the scan.
Network Countermeasures	4	Firewall blocks all of the UDP ports in the scan.
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 8

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
746991	18Mar2000	20:26:24	167.8.29.52	2714	dns.our.dmz	33434	udp	len 64
746992	18Mar2000	20:26:25	167.8.29.52	2715	dns.our.dmz	33434	udp	len 64
746993	18Mar2000	20:26:26	167.8.29.52	2716	dns.our.dmz	33434	udp	len 64
746994	18Mar2000	20:26:28	167.8.29.52	2717	dns.our.dmz	33434	udp	len 64
746995	18Mar2000	20:26:29	167.8.29.52	2718	dns.our.dmz	33434	udp	len 64
746996	18Mar2000	20:26:30	167.8.29.52	2719	dns.our.dmz	33434	udp	len 64
746997	18Mar2000	20:27:28	206.251.19.89	2811	dns.our.dmz	33434	udp	len 64
746998	18Mar2000	20:27:29	206.251.19.89	2812	dns.our.dmz	33434	udp	len 64
746999	18Mar2000	20:27:30	206.251.19.89	2813	dns.our.dmz	33434	udp	len 64
747000	18Mar2000	20:27:32	206.251.19.89	2814	dns.our.dmz	33434	udp	len 64
747001	18Mar2000	20:27:33	206.251.19.89	2815	dns.our.dmz	33434	udp	len 64
747002	18Mar2000	20:28:19	167.8.29.52	2714	dns.our.dmz	33434	udp	len 64
747003	18Mar2000	20:28:21	167.8.29.52	2715	dns.our.dmz	33434	udp	len 64
747004	18Mar2000	20:28:22	167.8.29.52	2716	dns.our.dmz	33434	udp	len 64
747005	18Mar2000	20:28:23	167.8.29.52	2717	dns.our.dmz	33434	udp	len 64
747006	18Mar2000	20:30:00	206.251.19.80	2711	dns.our.dmz	33434	udp	len 64
747007	18Mar2000	20:30:01	206.251.19.80	2712	dns.our.dmz	33434	udp	len 64
747008	18Mar2000	20:30:03	206.251.19.80	2713	dns.our.dmz	33434	udp	len 64
747009	18Mar2000	20:30:04	206.251.19.80	2714	dns.our.dmz	33434	udp	len 64
747013	18Mar2000	20:52:03	167.8.29.92	2814	dns.our.dmz	33434	udp	len 64
747014	18Mar2000	20:52:04	167.8.29.92	2815	dns.our.dmz	33434	udp	len 64
747015	18Mar2000	20:52:05	167.8.29.92	2816	dns.our.dmz	33434	udp	len 64
747016	18Mar2000	20:52:06	167.8.29.92	2817	dns.our.dmz	33434	udp	len 64
747017	18Mar2000	20:52:07	167.8.29.92	2818	dns.our.dmz	33434	udp	len 64
747018	18Mar2000	20:52:08	167.8.29.92	2819	dns.our.dmz	33434	udp	len 64
747019	18Mar2000	20:57:37	167.8.29.52	2714	dns.our.dmz	33434	udp	len 64
747020	18Mar2000	20:57:38	167.8.29.52	2715	dns.our.dmz	33434	udp	len 64
747021	18Mar2000	20:57:39	167.8.29.52	2716	dns.our.dmz	33434	udp	len 64
747022	18Mar2000	20:57:40	167.8.29.52	2717	dns.our.dmz	33434	udp	len 64
747023	18Mar2000	20:57:42	167.8.29.52	2718	dns.our.dmz	33434	udp	len 64
…	…	…	…	…	…	…	…	…
784682	29Mar2000	11:53:24	167.8.29.52	2714	dns.our.dmz	33434	udp	len 64
784683	29Mar2000	11:53:25	167.8.29.52	2715	dns.our.dmz	33434	udp	len 64
784684	29Mar2000	11:53:26	167.8.29.52	2716	dns.our.dmz	33434	udp	len 64
784685	29Mar2000	11:53:27	167.8.29.52	2717	dns.our.dmz	33434	udp	len 64
784973	29Mar2000	12:26:02	209.67.78.202	3409	dns.our.dmz	33434	udp	len 64
784974	29Mar2000	12:26:03	209.67.78.202	3410	dns.our.dmz	33434	udp	len 64
784975	29Mar2000	12:26:04	209.67.78.202	3411	dns.our.dmz	33434	udp	len 64
784977	29Mar2000	12:26:05	209.67.78.202	3412	dns.our.dmz	33434	udp	len 64
784978	29Mar2000	12:26:06	209.67.78.202	3413	dns.our.dmz	33434	udp	len 64
785222	29Mar2000	12:41:43	209.67.78.203	3309	dns.our.dmz	33434	udp	len 64
785223	29Mar2000	12:41:44	209.67.78.203	3310	dns.our.dmz	33434	udp	len 64
785224	29Mar2000	12:41:45	209.67.78.203	3311	dns.our.dmz	33434	udp	len 64
785225	29Mar2000	12:41:46	209.67.78.203	3312	dns.our.dmz	33434	udp	len 64
785227	29Mar2000	12:41:47	209.67.78.203	3313	dns.our.dmz	33434	udp	len 64

Existence: Many different IP addresses are visiting us.

History: There is no history of any of these addresses visiting our network before 3/18/00. Visitors from the same addresses or very close neighbors have been visiting ever since.

Techniques: All of the visitors in these detects have certain things in common. Every new visitor begins sending packets to UDP port 33434 of our DNS server. They send almost exactly one packet a second. Each IP address will send between 4 and 6 packets and then stop.

The most curious thing is the source ports used, and how they relate to the IP addresses. For example, 206.251.19.89 begins on 3/18/00 at 20:27:28 using a source port of 2811. Then, 2.5 minutes later, its neighbor 206.251.19.80 starts sending packets using a source port of 2711, a difference of exactly 100.

167.8.29.52 begins at 20:26:24 and again at 20:28:52 with a source port of 2714. At 20:52:03, its neighbor, 167.8.29.92 begins with a source port of 2814, again a difference of exactly 100. Then, so as not to be outdone, 167.8.29.52 returns 30 seconds after that, again beginning with source port 2714. That same address continued in the same manner until 3/29, the day the logs were queried for this report.

The same behavior of using a source port 100 away from your neighbor is repeated on 3/29/00 as 209.67.78.202 begins using a source port of 3409. Then, 15 minutes later, his next-door neighbor, 209.67.78.203 begins using port 3309. The fact that we have observed 3 instances of two hosts on the same subnet using source ports exactly 100 off is more than a coincidence.

Intent: The visitor is attempting to do a traceroute to our DNS server.

Targeting: Our DNS server is specifically being targeted in this scan.

Analysis: Some traceroute programs use UDP port 33434. It could be a server trying to determine the best route to get to our DNS server, but the fact that we saw no traffic to this port until 3/18/00 and then have seen it constantly ever since (and from a large number of hosts) is troubling. Also, a traceroute would generally be from the same source port and do incrementing destination ports, which is not the case here. It could be a network mapping attempt, or it could be a trojan that scans all public DNS servers.

The weird behavior with the source ports is hard to explain. It does indicate that the packets are being scripted and crafted. The difference of 100 between neighboring addresses could be explained by a visitor somewhere spoofing all of the IP addresses and changing the source port every time they change hosts. But that would not explain why we see the same IP address (167.8.29.52) always starts on the same source port. I cannot think of a good explanation for this.

Severity:

Component	Score	Comments
Criticality	4	Our DNS server is being targeted.
Lethality	3	It is unknown how the visitor would use any information gathered in this mapping attempt.
System Countermeasures	4	All operating systems are running the latest patches.
Network Countermeasures	4	Firewall blocks all packets with a destination port of UDP 33434
Severity Score	-1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

DETECT # 9

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
29940	17Aug1999	16:59:18	200.26.41.142	1887	10.10.1.1	12345	tcp	len 44
29941	17Aug1999	16:59:18	200.26.41.142	1888	10.10.1.2	12345	tcp	len 44
29942	17Aug1999	16:59:18	200.26.41.142	1889	10.10.1.3	12345	tcp	len 44
50936	25Aug1999	0:55:57	p31-term10-in.netdirect.net	2731	10.10.1.1	12345	tcp	len 48
50937	25Aug1999	0:55:57	p31-term10-in.netdirect.net	2734	10.10.1.2	12345	tcp	len 48
50938	25Aug1999	0:55:58	p31-term10-in.netdirect.net	2736	10.10.1.3	12345	tcp	len 48
317298	26Nov1999	18:27:55	98CA96FC.ipt.aol.com	1197	10.10.1.1	12345	tcp	len 48
317299	26Nov1999	18:27:55	98CA96FC.ipt.aol.com	1199	proxy.our.dmz	12345	tcp	len 48
317300	26Nov1999	18:27:55	98CA96FC.ipt.aol.com	1200	mail.our.dmz	12345	tcp	len 48
317301	26Nov1999	18:27:55	98CA96FC.ipt.aol.com	1201	dns.our.dmz	12345	tcp	len 48
423309	17Dec1999	17:14:46	208.33.12.129	1207	10.10.1.100	12345	tcp	len 48
423310	17Dec1999	17:14:46	208.33.12.129	1208	10.10.1.101	12345	tcp	len 48
423311	17Dec1999	17:14:46	208.33.12.129	1209	10.10.1.102	12345	tcp	len 48
423312	17Dec1999	17:14:46	208.33.12.129	1210	10.10.1.103	12345	tcp	len 48
423313	17Dec1999	17:14:46	208.33.12.129	1211	10.10.1.104	12345	tcp	len 48
507150	4Jan2000	16:12:32	208.33.12.120	1550	10.10.1.1	12345	tcp	len 48
507151	4Jan2000	16:12:32	208.33.12.120	1551	10.10.1.2	12345	tcp	len 48
507152	4Jan2000	16:12:32	208.33.12.120	1552	10.10.1.3	12345	tcp	len 48
507153	4Jan2000	16:12:32	208.33.12.120	1553	10.10.1.4	12345	tcp	len 48

Existence: Many different IP addresses are visiting us.

History: There is no other history of these hosts visiting our network. However, the last two scans, almost a month apart, are from the same class C subnet.

Techniques: The visitors are sending packets to every address on our class C network to TCP port 12345. All of the scans are very fast.

Intent: The intent is to find a server on our subnet that will respond on TCP port 12345.

Targeting: Our class C subnet is being targeted. In one of the scans, our mail, proxy, and DNS servers are targeted.

Analysis: The speed of these scans indicates that a script is being used. The packets do not appear to be crafted. This is a host scan looking for a host listening on TCP port 12345. Because the Netbus trojan is known to use this port, it is safe to conclude that this is a scan for this trojan.

The most interesting of these scans is the scan from 98CA96FC.ipt.aol.com – the other 4 locations were performing sequential host scans for port 12345, whereas this one only targeted our proxy, mail, and DNS servers without hitting any others. This indicates that this particular visitor has information about servers in our DMZ.

Severity:

Component	Score	Comments
Criticality	5	Specific machines are being targeted in at least one of the scans.
Lethality	5	Netbus is a very lethal vulnerability
System Countermeasures	4	All operating systems are running the latest patches.
Network Countermeasures	4	Firewall blocks all packets to TCP port 12345
Severity Score	2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

TRACE #10

ID	Date	Time	SourceIP	SourcePort	DestIP	DestPort	Proto	Info
107151	18Sep1999	6:44:07	cisco.cl.au.ac.th	1444	208.33.3.237	3128	tcp	len 48
108623	19Sep1999	16:22:17	pppt09-47.ght.iadfw.net	1036	208.33.3.226	3128	tcp	len 48
115393	22Sep1999	6:49:47	AOL3	61851	208.33.3.160	3128	tcp	len 44
123231	24Sep1999	5:51:58	r65h209.res.gatech.edu	1489	DMZ-PRX01	3128	tcp	len 44
123399	24Sep1999	6:27:57	202.54.33.206	63802	208.33.3.75	3128	tcp	len 44
133106	28Sep1999	0:10:46	cr838829-a.ktchnr1.on.wave.home.com	4669	208.33.3.88	3128	tcp	len 48
138128	29Sep1999	17:36:24	4.169.05.dn.dialup.cityline.ru	2376	DMZ-PRX01	3128	tcp	len 48
…	…	…	…	…	…	…	…	…
725494	11Mar2000	23:45:33	47.6.87.194.dynamic.dol.ru	2040	DMZ-PRX01	3128	tcp	len 48
768355	25Mar2000	2:36:14	ASHRAF	2555	208.33.3.173	3128	tcp	len 44

Existence: Many different IP addresses are visiting us.

History: We began seeing this type of traffic on 9/18/99 and are still seeing it today. There is no other history of any of these hosts visiting our network.

Techniques: Multiple visitors are sending TCP packets to port 3128. Each host is sending only one packet at a time, and they do not appear to return.

Intent: The visitor is looking for a host that will respond on port 3128.

Targeting: In some cases, it looks like it is a wildly random host scan of our class C subnet. In other cases, it looks like our proxy server is the target.

Analysis: This traffic is a result of hosts infected with the RingZero trojan. These infected hosts scan for port 3128, the squid proxy service, and report back to a central location.

Severity:

Component	Score	Comments
Criticality	5	Our proxy server is the target of this scan.
Lethality	3	It is unknown how the visitor would use any information gathered from this scan.
System Countermeasures	4	All operating systems are running the latest patches, and none are listening on TCP port 3128.
Network Countermeasures	4	Firewall blocks all ports destined for TCP port 3128.
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures