GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

GIAC Certified Intrusion Analyst
Practical Detects Assignment

Student Name: James Summers
Date: June 14, 2000

Notes About Detects:
All of these detects were taken from PIX firewall logs. The format of the logs was changed due to the use of an in house parsing tool to cut away the non-interesting messages.

Notes About The Traces:
The local IP addresses were cleansed. Therefore, the follow naming convention is used:

server.www -- Is the business' business critical Web Server.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 1

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-26	00:37:13	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:21	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:25	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:29	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:33	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:37	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:41	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP
2000-05-26	00:37:45	205.229.240.70	4804	server.www	161	udp		Deny inbound UDP

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

The probability of the source port being spoofed is very little. The attack it self would not work if the address was spoofed.

Description of Attack:

This attack is on udp port 161, which is the simple network management protocol (SNMP) port. SNMP can be used to get general and statistical information from a system or to configure a system or both. Because of the nature of SNMP this attack could be an information gathering attack or it could be an attack with the purpose of changing the configuration of the system it all depends on what community password the attacker is trying. By default SNMP uses “public” as the read only password and “private” as the read/write password. Note that we cannot tell from this trace because we do not have the data for the individual packets.

Attack Mechanism:

This is a general request to see if a system will respond to an SNMP request.

Correlations:

Scanning for open SNMP ports on servers is a well-known information gathering technique. Stephen Northcutt discussed this at the SANS2000 Intrusion detection class held in San Jose and the relate material is in the courseware manual, “2.5 Intrusion Detection Workshop” page 285.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	2	SNMP can give away a lot of useful information.
System Countermeasures	4	The system is running the latest security patches and snmp passwords are not the default.
Network Countermeasures	4	Firewall blocks all packets to udp port 161 by default
Severity Score	-1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall. Also the SNMP passwords have been changed from the defaults.

Multiple Choice Test Question:

Most SNMP scans are:

a) Information gathering
b) Used to detect trojans
c) TCP mapping
d) UDP port mapping

Answer: A

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 2

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-30	00:23:16	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
2000-05-30	00:23:18	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
2000-05-30	00:23:36	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
2000-05-30	00:23:37	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
…								
2000-05-30	00:28:40	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
2000-05-30	00:28:44	202.105.182.26	137	server.www	137	udp		Deny inbound UDP
2000-05-30	00:28:45	202.105.182.26	137	server.www	137	udp		Deny inbound UDP

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

My log files are full of hundreds of similar traces with differing source ip addresses all only attacking one system. This leads me to think denial of Service (DoS) attack thus the source IP could be spoofed. But they may not be if the traces are really for information gathering.

Description of Attack:

As stated above there are numerous traces of this nature in a single days log, if this was a information gathering scan on the NetBios Name Services then why have 50 to 60 scans to the same server. So, I think that this is a DoS.

Attack Mechanism:

Attacker is either spoofing addresses or is really stupid and is trying to do an information gathering scan but wants to make really sure they can't get the nbtstat information.

Correlations:

Stephen Northcutt discussed the information gathering scan at the SANS2000 Intrusion detection class held in San Jose and the relate material is in the courseware manual, "2.5 Intrusion Detection Workshop" page 292-295. However, I have not been able to get more information to prove or disprove a DoS.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	3	The NetBios Name Service can give away a lot of useful information.
System Countermeasures	3	The system is running the latest security patches.
Network Countermeasures	4	Firewall blocks all packets to udp port 137 by default
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall.

Multiple Choice Test Question:

What operating systems have to be concerned with this attack?

a) Windows NT
b) Windows 2000
c) Unix
d) All the above

Answer: D because of samba on Unix.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 3

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-26	11:31:26	132.197.114.187	2127	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-05-26	11:31:29	132.197.114.187	2127	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-05-26	11:31:35	132.197.114.187	2127	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-05-26	11:31:47	132.197.114.187	2127	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-06-06	07:39:51	132.197.114.187	2056	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-06-06	07:39:54	132.197.114.187	2056	server.www	7001	tcp	SYN	Inbound TCP connection denied
2000-06-06	07:40:00	132.197.114.187	2056	server.www	7001	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

For the attack to work you would not want a spoofed address, therefore the probability of the source address being spoofed is low.

Description of Attack:

This is a scan looking for a host listening on tcp port 7001, which is a known port for Freak88.

Attack Mechanism:

Freak88 is a windows trojan that infects a system. Once infected Freak88 auto starts from the registry and copies itself to c:\windows\system at this time the system will be listening on port 7001. The system is now available to be used by an attacker for denial of service (DoS) attacks on other systems.
http://home.cyberarmy.com/freak88/

Correlations:

The destination port of 7001 gives this scan a definite fingerprint. This is a scan looking for a host listening on tcp port 7001. Because the Freak88 trojan is known to use this port, it is safe to conclude that this is a trojan scan for the Freak88 trojan.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	2	If the system was infected with the Freak88 it could be used for DoS attacks by the attacker.
System Countermeasures	5	The system is running the latest security patches and the system has the latest virus definitions updated nightly.
Network Countermeasures	4	Firewall blocks all packets to port 7001 by default
Severity Score	-2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall and the system has antivirus software that is updated nightly.

Multiple Choice Test Question:

The above attack is a
a) DoS attack
b) Portmapper attack
c) Scaning for trojan
d) None of the above

Answer: C

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 4

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-28	14:35:18	198.104.23.111		Server.www				Deny IP – IP options 0x94040000
2000-05-28	14:35:57	198.104.23.111		Server.www				Deny IP – IP options 0x94040000
2000-05-28	14:36:08	198.104.23.111		Server.www				Deny IP – IP options 0x94040000
2000-05-29	23:40:00	136.207.63.240		Server.www				Deny IP – IP options 0x94040000
2000-05-29	23:40:07	136.207.63.240		Server.www				Deny IP – IP options 0x94040000
2000-05-29	23:40:18	136.207.63.240		Server.www				Deny IP – IP options 0x94040000

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

Along with the above address I have traces of the same type from the 69th Army Signal Battalion (136.207.63), Single Agency Manager (140.185.62.62), US West (216.1660.22.85), Korea Network Information Center (211.44.83.88) and others. I do not believe that these address have been spoofed.

Description of Attack:

The firewall dropped these packets because of the IP options being set. The firewall drops all packets with the IP options set.

Attack Mechanism:

There are known problems with some firewalls locking up when IP options are set. It is just a matter of these options not being used often so many TCP/IP stacks do not know how to handle them.

Correlations:

As for this IP option, it is the IP Router Alert option. The option type is to alert transit routers to more closely examine the contents of an IP packet. This is useful for new protocols that are addressed to a destination but require relatively complex processing in routers along the path; protocols like RSVP and IGMPv2. This is all laid out in rfc2113. http://www.cis.ohio-state.edu/htbin/rfc/rfc2113.html

The questions are why is my firewall seeing these packets and could they be harmful in some way.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	1	The web servers ignored these packets.
System Countermeasures	4	The operating system is running the latest security patches.
Network Countermeasures	4	Firewall drops all packets with the IP Options set
Severity Score	-2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall.

Multiple Choice Test Question:

At what byte in the IP Header does the IP options start

a) 8th byte
b) 16th byte
c) 10th byte
d) 20th byte

Answer: D

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 5

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-26	06:27:09	161.22.134.54	1059	Server.www	524	tcp	SYN	Inbound TCP connection denied
2000-05-26	06:27:12	161.22.134.54	1059	Server.www	524	tcp	SYN	Inbound TCP connection denied
2000-05-26	06:27:18	161.22.134.54	1059	Server.www	524	tcp	SYN	Inbound TCP connection denied
2000-05-30	00:45:32	161.22.134.54	1069	Server.www	524	tcp	SYN	Inbound TCP connection denied
2000-05-30	00:45:35	161.22.134.54	1069	Server.www	524	tcp	SYN	Inbound TCP connection denied
2000-05-30	00:45:41	161.22.134.54	1069	Server.www	524	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

The probability of the source address being spoofed is not very likely. Although, the source address is accessible by the Internet the fact that this trace is happening every few days one time a day makes the likely hood rare.

Description of Attack:

The attack is checking to see if our web server is listening on tcp port 524, which is Netware Core Protocol (NCP) for Netware 5 only.

http://www.connectotel.com/border/bmports.html

Attack Mechanism:

This is a general request to see if a system will respond on a port.

Correlations:

The Netware Core Protocol (NCP) was developed by Novell to be used by a Novell Netware client to request network services (file and print sharing) from a Netware server. NCP originally ran over IPX however, with the advent of Netware 5 Novell ported the protocol to run over IP on tcp port 524.

http://developer.novell.com/research/appnotes/1992/december/04/02.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	3	On a Netware 5.0 Server this can be used to get share information.
System Countermeasures	5	The system is running the latest security patches and is not listening on port 524.
Network Countermeasures	4	Firewall blocks all packets to tcp port 524 by default
Severity Score	-1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall. It is always good to know what tcp and udp ports your servers use and disable all unused ports on your servers. A program like nmap can be used to see which ports are open on your server.

Multiple Choice Test Question:

Novell Netware's Netware Core Protocol (NCP) run's on

a) IPX
b) TCP/IP
c) ICMP
d) A & B

Answer: D

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 6

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-05-27	10:24:25	192.60.155.87	1055	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:24:28	192.60.155.87	1055	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:24:34	192.60.155.87	1055	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:23:47	192.60.155.87	1055	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:25:28	192.60.155.87	1056	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:25:31	192.60.155.87	1056	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:25:37	192.60.155.87	1056	server.www	139	tcp	SYN	Inbound TCP connection denied
2000-05-27	10:25:50	192.60.155.87	1056	server.www	139	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

In this case the attacker is either scanning looking for NetBIOS Session Services or more likely, this is an out of band denial of service (DoS) attack. In either case the probability of spoofing would be low.

Description of Attack:

This is a Winnuke attack against a Windows NT system. The best port to do Winnuke against seems to be the NetBIOS Session Services port, 139.

Attack Mechanism:

The Winnuke attack is done by sending OOB [Out Of Band] data to an established connection you have with a windows user, thus difficult to be a spoofed address. However Windows doesn't understand the OOB data and does crazy things and could go as far a locking up. Reboot is needed.

http://rootshell.com/archive-j457nxiqi3gq59dv/199707/winnuke.c.html

Correlations:

Normally you do not see traffic to or from port 139 from outside networks unless there is a Windows trust established. And since there are no trusts setup, I believe this is a Winnuke attack.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	4	This attack could force the system to be rebooted.
System Countermeasures	4	The system is running the latest security. However NetBIOS is running.
Network Countermeasures	4	Firewall blocks all packets to tcp port 139 by default
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall. If you can help it, don't allow NetBIOS to travel outside of your network. Furthermore, if you can, kill all NetBIOS off you network and the associated ports (135-139) from your systems.

Multiple Choice Test Question:

The above trace is characteristic of what attack?

a) PingODeath
b) Smurf
c) Winnuke
d) Sniff-IT

Answer: C

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 7

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-06-04	09:40:36	200.241.255.21	4781	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	09:40:42	200.241.255.21	4781	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	09:59:15	200.241.255.21	1768	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	09:59:18	200.241.255.21	1768	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	09:59:24	200.241.255.21	1768	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	10:06:35	200.241.255.21	3011	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	10:06:38	200.241.255.21	3011	server.www	515	tcp	SYN	Inbound TCP connection denied
2000-06-04	10:06:44	200.241.255.21	3011	server.www	515	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

The probability that the source port was spoofed is little to none. There is no advantage for spoofing for the attack is not a denial of service (DoS).

Description of Attack:

The address resolves to pm3-03-s20.interconect.com.br, which in most cases is a Livingston Postmaster 3 dial up access switch. I looks like someone from Britain would like to see if I am running the spooler print service. Maybe the want to send me a quick note.

Attack Mechanism:

This is either a general request to see if a system has the spooler port open or this is just a misconfigured system.

Correlations:

RFC 1179. Port 515 should be used for all printing jobs. New printers come with internal print servers that could be susceptible to an attack on this port. These printers also tend to have local route information along with the ability to be remotely configured.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	1	Go for very general information gathering.
System Countermeasures	4	The system is running the latest security patches and is not running the spooler service.
Network Countermeasures	4	Firewall blocks all packets to tcp port 515 by default
Severity Score	-2	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall.

Multiple Choice Test Question:

What is tcp port 515 used for?

a) TFTP
b) Print Spooler
c) SUN RPC
d) SMTP

Answer: B

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 8

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-06-05	17:03:48	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:03:51	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:03:57	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:03:58	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:04:01	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:04:07	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:04:09	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied
2000-06-05	17:04:19	64.81.1.66	62741	server.www	2301	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

For the attack to work you would not want a spoofed address, therefore the probability of the source address being spoofed is low.

Description of Attack:

The intent is to see if server.www will respond to an http request to tcp port 2301, which is the Compaq Insight Manager Web port. Compaq Insight Manager is an application that runs on Compaq Proliant servers and shows all information about the Compaq hardware and OS. Revision levels, IP addresses, BIOS version, etc.…

Attack Mechanism:

This is a general http request, http://server.www:2301, to see if a system will respond to the request. If the system responds then try the default logons; however by default the anonymous user has full access to all the information and there is a lot.

Correlations:

All the information about the Compaq Insight Manager can be looked up online at www.compaq.com.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	4	The web agent will allow you to reboot the system and change ip's.
System Countermeasures	1	The system is running the latest security patches; however, the Insight Manager default settings were in place.
Network Countermeasures	4	Firewall blocks all packets to tcp port 2301 by default
Severity Score	4	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses were adequate to stop the attack for the attack was blocked by the firewall. However, all default passwords were modified and the anonymous user was removed.

Multiple Choice Test Question:

What byte offset in the tcp header would the port 2301 be at in the above trace?

a) 10
b) 16
c) 4
d) 8

Answer: B

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 9

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-06-07	10:55:28	128.173.105.121	2373	server.www	53	tcp	SYN	Inbound TCP connection denied
2000-06-07	10:55:31	128.173.105.121	2373	server.www	53	tcp	SYN	Inbound TCP connection denied
2000-06-07	10:55:37	128.173.105.121	2373	server.www	53	tcp	SYN	Inbound TCP connection denied

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

For the attack to work you would not want a spoofed address, therefore the probability of the source address being spoofed is low.

Description of Attack:

The intent is to see if 192.168.11.220 will respond to a request to tcp port 53 (DNS Zone Transfer).

Attack Mechanism:

The attack tries to connect to a DNS server to request that the DNS server send all zone information for x domain. This is an information attack but can easily lead into a situation were the attacker could take control or your domain name server.

Correlations:

Stephen Northcutt discussed this at the SANS2000 Intrusion detection class held in San Jose and the relate material is in the courseware manual, “2.5 Intrusion Detection Workshop”.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	4	This attack is an informational attack but there are some vulnerabilities in some DNS servers where an attack could get root access.
System Countermeasures	5	The system is running the latest security patches and the server is not running DNS services.
Network Countermeasures	4	Firewall blocks all packets to tcp port 53 by default
Severity Score	0	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall. Also, the server being attacked is not running DNS services.

Multiple Choice Test Question:

TCP Port 53 is use for?

a) DNS Zone Transfers
b) POP2
c) DNS Look ups
d) Both A & C

Answer: D

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect # 10

Date	Time	Source IP	Source Port	Dest IP	Dest Port	Proto	Flags	Error Message
2000-06-06	16:02:50	212.162.132.192	60000	server.www	2140	udp		Deny inbound UDP

Source of Trace:

My network.

Detect By:

Firewall.

Probability Source Address Spoofed:

For the attack to work you would not want a spoofed address, therefore the probability of the source address being spoofed is low.

Description of Attack:

This scan is looking for a host listening on port 2140; which is a known port for DeepThroat.

Attack Mechanism:

DeepTrhoat is the hidden (hacker's) remote administration utility used to control remote workstations similar to Backdoor.BO (aka Back Orifice) trojan. Once on your system an attack need only attach to port 2140 to then be able to remote control your system.

Correlations:

The udp source port of 60000 gives this scan a definite fingerprint. That, combined with the destination port of 2140, it is safe to conclude that this is a trojan scan for the DeepThroat trojan. http://www.avpve.com/viruses/backdoor/deepthro.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity:

Component	Score	Comments
Criticality	5	This web server is mission critical to the business.
Lethality	5	If on the system, DeepThroat will allow an attack to remotely control the system.
System Countermeasures	5	The system is running the latest security patches and the latest virus definitions are updated nightly passwords are not the default.
Network Countermeasures	4	Firewall blocks all packets to tcp port 2140 by default
Severity Score	1	Severity = (Criticality + Lethality) – (system countermeasures + net countermeasures

Defensive Recommendation:

Defenses are fine; attack was blocked by the firewall. Definitely want to keep the virus code up to date by updating definitions nightly.

Multiple Choice Test Question:

Why is the lethality of the DeepTroat tojan so high?

a) Attacker has access to passwords.
b) Attacker has ability to deny service to the system.
c) Attacker has the ability to gain administrative rights across the net.
d) All the above

Answer: D

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.