Port Scanning is not always what it seems.
By Darin W. Powell

Abstract. Daily electronic data transfer over the Internet is essential in today's business environment. The use of the Internet for this transfer makes corporations vulnerable to hacker attacks. To be aware of the attacks, intrusion detection systems are essential. The top market share for intrusion detection systems is owned by Cisco called Cisco Secure Intrusion Detection System (Cisco Secure IDS). The key features of the Cisco Secure IDS are its dynamic response capabilities, scalability and performance, and its security visibility. These features give the client the ability to detect port scans – one of the major attacks that hackers make. The interesting point here is that – a port scan (a perceived intrusion) may not be what it appears.

Here is the scenario:

There are three major features of Cisco Secure IDS.

1 - Dynamic Response Capability - Cisco Secure IDS uses the dynamic response capability to check the user Internet entries and either forwards them to their location or the system can automatically shun or block them. The dynamic response feature is done in real-time and is customizable by using and modifying access control lists on the router on the fly. The dynamic response could then detect and potentially block unauthorized activity thus protecting your network from real-time and future attack.

2 – Scalability - The scalability and performance feature allows for security from a central management monitor. Through the use of HP Openview as a graphical user interface, corporations can centrally monitor all traffic from Cisco sensors across their wide area network. Also, by consolidating management costs, the Cisco Secure IDS can save personnel costs as well as provide a better overall picture of the security of the network.

3 - Security visibility can be used to better inform management through the use of placing the alarm information into a central database and generating graphs, reports, and event logs. The database can be an excellent tool for historical data and trend analysis.

Cisco Secure IDS Installation/Configuration

One of the big questions with installing an intrusion detection system is the placement of the Cisco Secure IDS. An administrator can place the Cisco Secure IDS inside or outside the firewall. There are pros and cons to each selection. The administrator can place a Sensor in both locations which is advantageous but the cost if of course higher.

If you place the sensor on the outside of the firewall, the sensor can monitor all incoming/outgoing network traffic. The problem is that the Sensor is not protected since it is outside the firewall. The other alternative is to place the Sensor inside the firewall. By placing the Sensor inside the firewall, the Sensor is secure, but it does not monitor all network traffic. The firewall will filter incoming traffic before it gets to the Sensor. The following diagram (Fig 1) shows the configuration of the devices for this example. The Cisco Secure IDS sits on the inside of the firewall for protection from scanning.

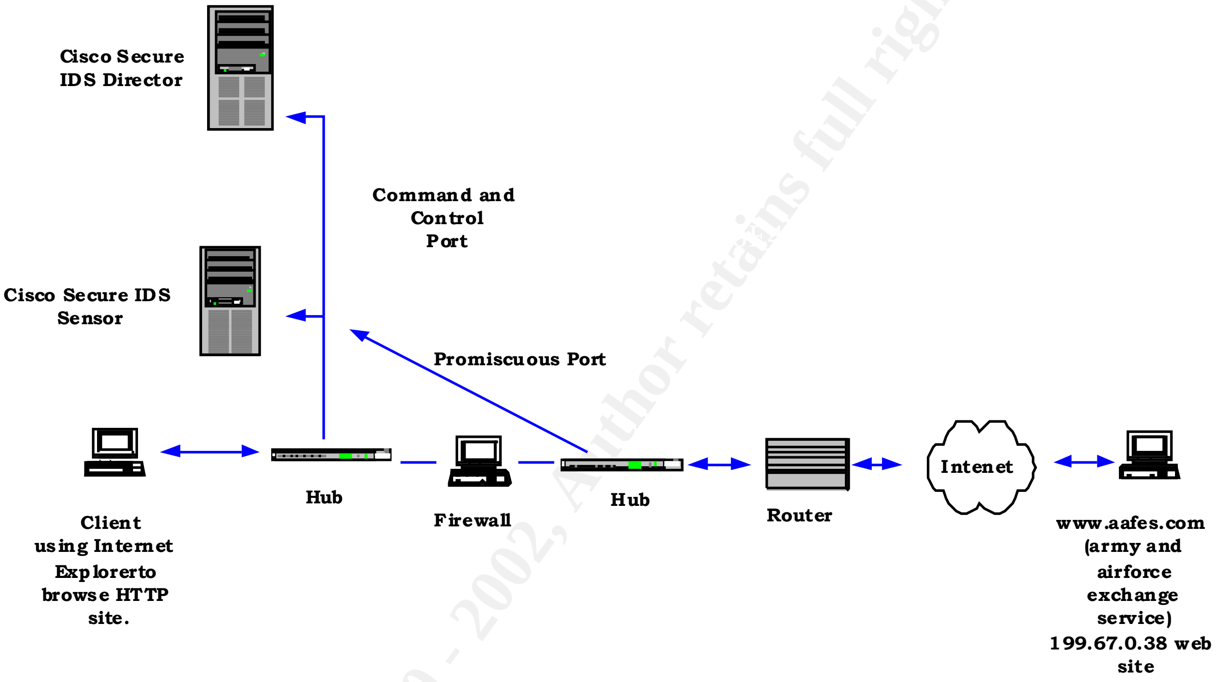

Cisco Secure IDS Director
Command and Control Port
Cisco Secure IDS Sensor
Promiscuous Port
Client using Internet Explorerto browse HTTP site.
Hub
Firewall
Hub
Router
Intenet
www.aafes.com (army and airforce exchange service) 199.67.0.38 web site

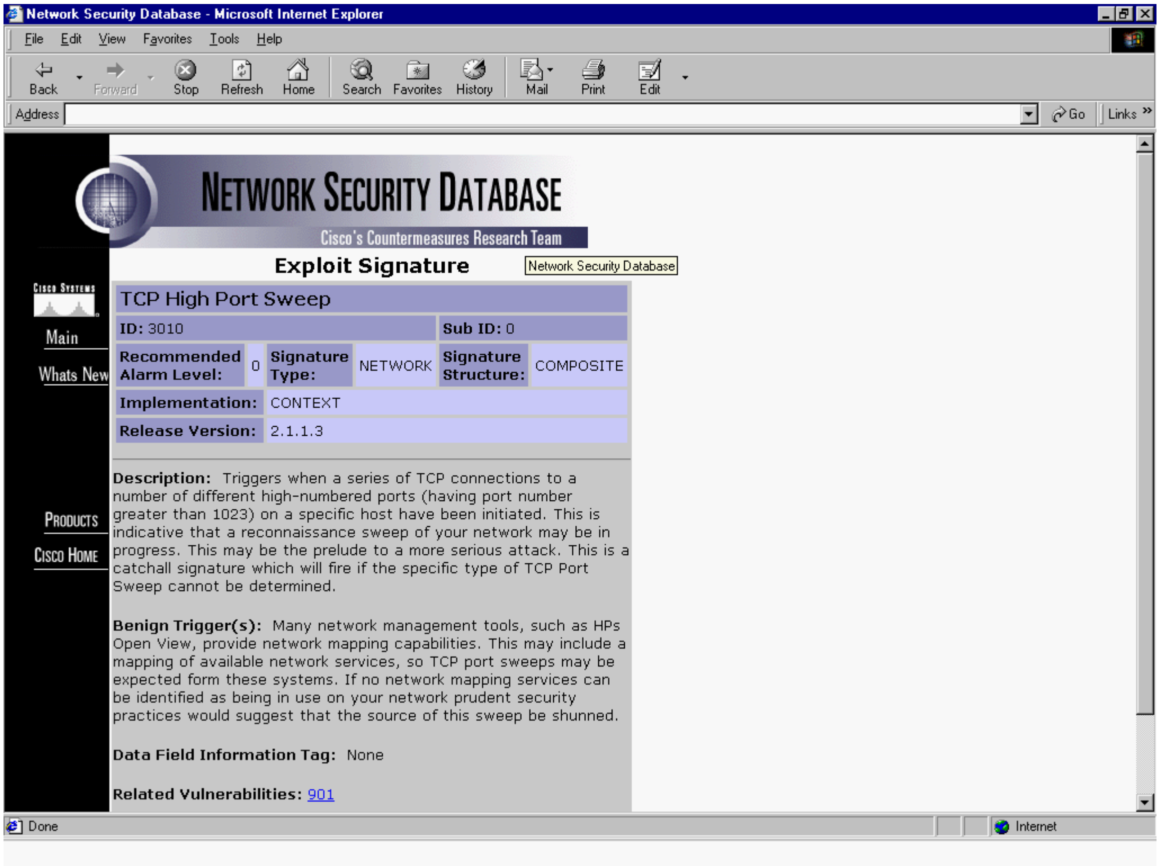
Figure 1. Network Diagram of example with Cisco Secure IDS (formerly known as NetRanger)

With this configuration, HP Openview (www.openview.hp.com) reported numerous TCP High Port Sweeps 3010 on the Cisco Secure IDS. The first step is to research who, what, when, and how.

An intrusion detection system normally identifies security occurrences by signature. A signature is a predefined event that once duplicated will signal an alarm. One of the signatures it looks for is a TCP high port scan. Today, most hackers will look to first identify your system and then scan for vulnerabilities and weaknesses using a port scan. One of the first things a hacker does is analyze and gather as much information about your network as possible. Once the hacker has a layout of your network, they can start attacks against known vulnerabilities. However, a port scan is not always what it seems.

At Christmas time, users go online to research products and make purchases. During this time, the port scan signature kept on coming up with signature 3010- High TCP Port Sweep on the HP Openview screen. Using the Cisco web page to check severity level and descriptions (Figure-3 the Cisco alarm definition and details) you can then research what the alarm actually means.

After getting numerous alarms, I looked up the problem in the detail section of the alarm. I used the Cisco web page to look up the signature to check the severity level and the description of the alarm 3010 (Figure-3 the Cisco alarm definition and detail).


Network Security Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Address
Go
Links
NETWORK SECURITY DATABASE
Cisco's Countermeasures Research Team
Network Security Database
Cisco Systems
Main
Whats New
Products
Cisco Home
Done
Internet

Exploit Signature

TCP High Port Sweep

ID: 3010				Sub ID: 0	
Recommended Alarm Level:	0	Signature Type:	NETWORK	Signature Structure:	COMPOSITE
Implementation:	CONTEXT				
Release Version:	2.1.1.3				

Description: Triggers when a series of TCP connections to a number of different high-numbered ports (having port number greater than 1023) on a specific host have been initiated. This is indicative that a reconnaissance sweep of your network may be in progress. This may be the prelude to a more serious attack. This is a catchall signature which will fire if the specific type of TCP Port Sweep cannot be determined.

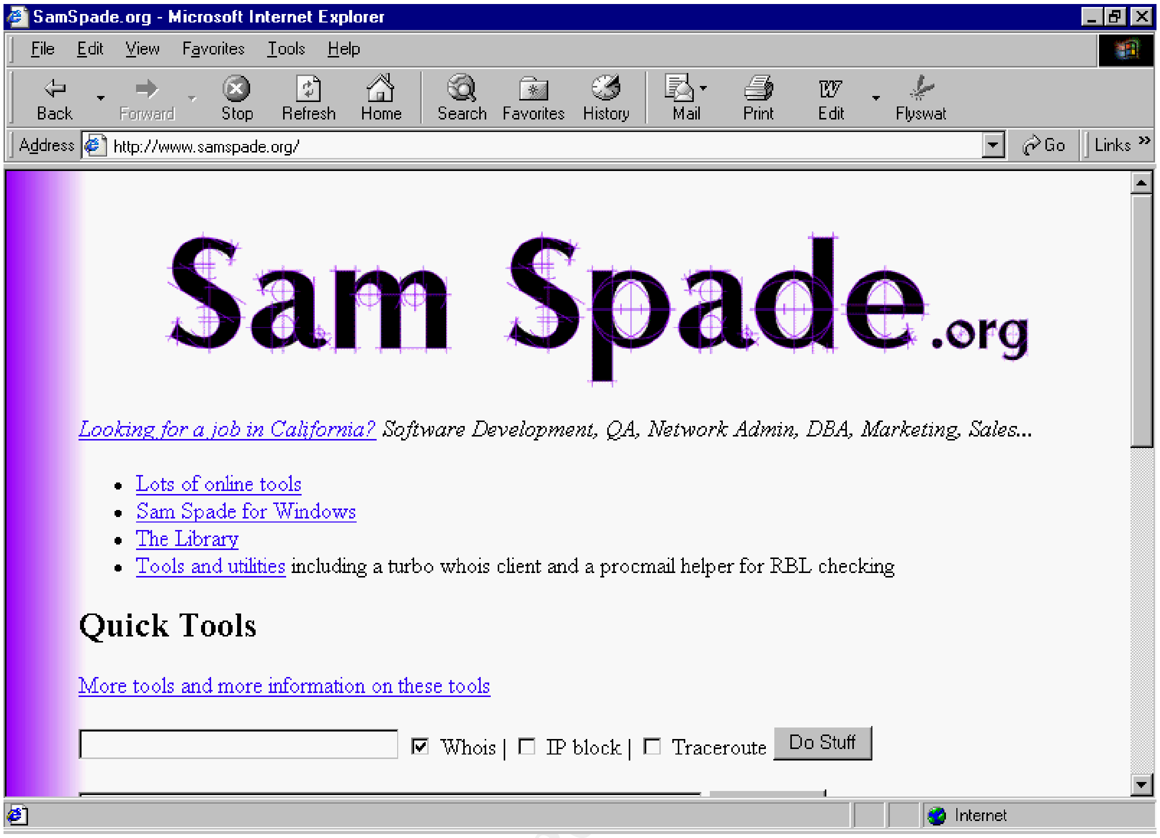
Benign Trigger(s): Many network management tools, such as HPs Open View, provide network mapping capabilities. This may include a mapping of available network services, so TCP port sweeps may be expected form these systems. If no network mapping services can be identified as being in use on your network prudent security practices would suggest that the source of this sweep be shunned.

Data Field Information Tag: None

Related Vulnerabilities: 901

Figure 3. Cisco Network Security Database 3010 exploit signature for a TCP High Port Sweep.

With the use of the Internet, intrusion detection can utilize the web to verify and track real alarms and differentiate the alarms from normal usage. The destination address from the alarm can be tracked down using www.samspade.org, www.nic.com, www.nic.mil, or by typing in the address on the browser address line. Once you enter the Sam Spade web site (refer to Figure 4), type the IP address in the box, put a check in the Whois and IP Block boxes, and hit the Do Stuff button and the web site will provide the requested information. If you are looking for an IP address and you only have the web site name, type the web site name in the box, put a check in the Whois box, and hit the button Do Stuff. The web site will provide the requested IP address.



http://www.samspade.org/

Sam Spade.org

Looking for a job in California? Software Development, QA, Network Admin, DBA, Marketing, Sales...

- Lots of online tools
- Sam Spade for Windows
- The Library
- Tools and utilities including a turbo whois client and a procmail helper for RBL checking

Quick Tools

More tools and more information on these tools

☑ Whois | □ IP block | □ Traceroute | Do Stuff

Figure 4. www.samspade.org screen capture

Once the web address or requested information is found, you can verify if there is something wrong that needs to be investigated further. Figure 5 shows a detailed log of what an administrator can obtain from the Cisco Secure IDS log file when incorporated into a Microsoft Excel spreadsheet. In this example, users were going to aafes.com to purchase Christmas gifts from the Army and Air Force Exchange Service web site. In this case, there was no intrusion attempt. The user just requested information and the web site returned the information on the next available port.

3010 Alarm Log

Date	Time	App ID	Sensor ID	Org ID	Alarm Level	TCP High Sweep	Port	Packet	Src IP	Dest IP	S Port	D Port
1/12/01	6:54:18	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2907
1/12/01	7:17:29	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	1854
1/12/01	7:46:54	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2167
1/12/01	7:47:07	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2695
1/12/01	7:48:10	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3005
1/12/01	7:48:11	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2476
1/12/01	7:48:54	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2662
1/12/01	7:50:52	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3851
1/12/01	7:50:52	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3321
1/12/01	7:51:33	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4207
1/12/01	7:52:51	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4789
1/12/01	7:52:52	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4266
1/12/01	7:54:28	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	1370
1/12/01	7:54:55	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4820
1/12/01	7:55:26	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	1512
1/12/01	7:58:08	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2640
1/12/01	7:58:35	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2244
1/12/01	7:59:05	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3152
1/12/01	7:59:46	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2792
1/12/01	8:00:48	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3231
1/12/01	8:01:18	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3911
1/12/01	8:01:22	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3549
1/12/01	8:02:14	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4367
1/12/01	8:02:15	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3849
1/12/01	8:03:02	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4195
1/12/01	8:03:04	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4733
1/12/01	8:04:49	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	4758
1/12/01	8:05:45	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	1967
1/12/01	8:06:20	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2039
1/12/01	8:06:33	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	2662
1/12/01	8:08:54	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3825
1/12/01	8:08:54	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	443	3277
1/12/01	8:15:44	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	2843
1/12/01	8:16:14	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	3136
1/12/01	8:18:14	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	4185
1/12/01	8:21:08	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	1970
1/12/01	8:25:20	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	3651
1/12/01	8:26:02	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	4010
1/12/01	8:27:12	10008	11	100	3		3010	TCP/IP	x.x.x.x	x.x.x.x	80	4476

Figure 5. 3010 Alarm Log signature pulled out of the Cisco SIDS Logs and pulled into Microsoft Excel.

As stated in the SANS conference, know your system. By knowing what your users are doing and how the system works, an administrator can eliminate false positives in intrusion detection. In this specific case, the users were going out on a specified port through the firewall. Once they connected to the web-site, www.aafes.com in this case (199.67.0.38), the users browsed and checked for product quantity, price, and availability. Once the user made this request, the web site would search through its database and send back an acknowledgement of the request. The problem was that the acknowledgement did not come back on the same port. The web site would perform a TCP high port scan until it located an available port to send the requested information back to the user.

This example illustrates how a port scan would not always be what it seemed. In most cases, port scanners are being used to gather information and look for vulnerabilities. In this case, the user requested information from a foreign web site and the web site was responding to the request.

In Summary

In today's Internet driven world, businesses are being pushed into being connected to the Internet. Due to the risk of being on the Internet, companies must show due diligence by placing firewalls in front of their networks to provide a security perimeter. Even with a firewall, it is exceptionally difficult to tell what is transpiring on the network wire without help. Intrusion detection systems assist an administrator in gaining more knowledge about what is happening on the wire. Knowing your system is a key phrase that is mentioned at SANS (www.sans.org) and is a good one. If you know more than your opponent, than you have a fighting chance. The example used here illustrates how knowing your system can alleviate some of the misconceptions about port scanning and how you can eliminate the need to research this type of event in the future. This example can also assist administrators on the setup, flexibility, and multiple features and configurations that can help in detecting intrusions. By knowing and configuring your system properly, business communication's risk on the Internet can be minimized and set to an acceptable level.

References.

1. Cisco Corporation. Product section of web site. URL: http://www.Cisco.com (03/01/01).

2. SamSpade Organization. Homepage URL: http://www.samspade.org/alerts (03/01/01).

3. Hewlett Packard. HP Openview 2001. URL: http://www.openview.hp.com (03/01/01).

4. Network Information Center. URL: http://www.nic.mil (03/01/01).

5. Army and Airforce Exchange Service. URL: http://www.aafes.com (03/01/01).

6. SANS Organization. URL: http://www.sans.org (03/01/01).

7. Network Information Center. URL: http://www.nic.com (03/01/01).