Global Information Assurance Certification Paper

Implementing and Subverting Cisco's Port Security

David J Kyger
MCSE

There was a time when, if you placed your network card into promiscuous mode, you could easily capture all clear text passwords on the network. Network switches have addressed this problem and is one of the reasons why many environments have replaced their aging hubs with switching devices. An additional security enhancement that switches provide is the ability to restrict hosts to using specific ports on the network. This feature, known as port security, restricts access to a port based on the host's Mac address.

There may be times on your network when you have to control what machines are allowed to be patched into your network The scenarios are many and could range from monitoring the activity of a lab to restricting the use of stray hubs on the network. This paper will explain how to implement this security feature on a Cisco switch as well as how to circumvent it.

This paper is divided into three primary exercises:
1) We will begin by enumerating data from a machine operating Windows NT workstation.
2) From there we will move on to a Cisco catalyst switch and illustrate how to enable, verify and disable port security.
3) Lastly, a step-by-step method on how to circumvent a port security enabled switch will be presented. This exercise will be performed with a host operating Windows NT 2000.

The convention will be as follows: commands typed at the prompt will be in bold and the output will be in italics. We will begin our exercise by trying to obtain the host's IP address.

*C:\WINNT>***tracert stag-beetle**
Tracing route to STAG-BEETLE [192.168.0.55] over a maximum of 30 hops:
1 <10ms <10ms <10ms anysite.anywhere.com [192.168.0.1]
2 <10ms <10ms <10ms STAG-BEETLE [192.168.0.55]
Trace complete

(Note: The command ping –a "host-name" can also be used to obtain the IP address)

We have just successfully utilized a command to derive the host's IP address. With this IP we can then jump to our next useful command, NBTSTAT.

*C:\WINNT>***nbtstat -A 192.168.0.55**

NetBIOS Remote Machine Name Table

Name Type Status

```
---------------------------------------------
STAG-BEETLE     <00>  UNIQUE      Registered
STAG-BEETLE     <20>  UNIQUE      Registered
GALAPAGOS       <00>  GROUP       Registered
GALAPAGOS       <1C>  GROUP       Registered
GALAPAGOS       <1B>  UNIQUE      Registered
STAG-BEETLE     <03>  UNIQUE      Registered
GALAPAGOS       <1E>  GROUP       Registered
GALAPAGOS       <1D>  UNIQUE      Registered
DKYGER          <03>  UNIQUE      Registered

MAC Address = 00-02-02-23-19-2a
```

From this we can gather some very useful information. The numbers that you see in the output are in hex and are referred to as NetBIOS suffixes. From suffix 03 we can derive that DKYGER is logged into the host machine STAG-BEETLE. Other useful information includes the domain name and other services the host may be currently offering. For a more comprehensive listing of NetBios Suffixes follow the URL cited at reference 1. For our purposes, however, we will focus on the information that we need to implement port security, specifically the host's Mac address. Now, having obtained this Mac address, we can move on to operate the switch.

Cisco switches utilize a database to store all Mac addresses, VLAN Ids and ports. This information is held in SRAM on a device known as a Supervisor Engine. This database is available and can be queried on the switch. The following command provides for us a convenient Mac address to port number association.

```
Console> (enable) show cam 00-02-02-23-19-2a
* = Static Entry. + = Permanent Entry. # = System Entry.

VLAN Dest MAC/Route Des  Destination Ports or VCs
---- -----------------  ---------------------------------------------------
1    00-02-02-23-19-2a   12/19
Total Matching CAM Entries Displayed = 1
```

For those who are unfamiliar with the port numbering scheme, here is a quick explanation. Each switch has a number of modules. These modules are placed in the switch and are numbered from top to bottom. Each module will have a certain number of ports. Ports are numbered from left to right. The command for querying a specific port is command mod_num/port_num. From our example, we can derive that the machine with Mac address 00-02-02-23-19-2a is physically patched into 12/19 (the 19th port in the 12th module). I have found that this tactic has saved me a lot of walking, as I do not have to visit the host in question to trace the path from the host to the switch.

Having gathered this information, we would like to check the status of this port. The following command will inform us as to whether port security is currently enabled for this device.

Console> (enable) **show port 12/19**

Port	*Name*	*Status*	*Vlan*	*Level*	*Duplex*	*Speed*	*Type*
12/19		*connected*	*1*	*normal*	*a-full*	*a-100*	*10/100BaseTX*

Port	*Security*	*Secure-Src-Addr*	*Last-Src-Addr*	*Shutdown*	*Trap*
12/19	*disabled*			*No*	*enabled*

This command provides such information as VLAN assignment, duplex mode and speed. More importantly, we want to know the status of port security for the device using port 12/19. From here we can see that port security is not currently enabled for this port. Also at this point there is no information detailing what Mac addresses have been accessing this port. The next block will show the command sequence and output after applying port security.

Console>(enable) **set port security 12/19 enable 00-02-02-23-19-2a**
Port 12/19 port security enabled with 00-02-02-23-19-2a as the secure mac address

Here we have applied port security for port 12/19 with the specified Mac address of 00-02-02-23-19-2a. At this point, only the host with the permitted Mac will be able to access the network through port 12/19. From this point forward or until port security is disabled, if this port is tampered with, i.e. the machine is unplugged and another machine is plugged in, the port will be disabled effectively stopping any traffic from being transmitted or received via this port.

The next command is used to display the current configuration for port 12/19. Notice the status of this port. Currently it is shut down. If we refer to Secure-Src-Addr and Last-Src_Addr we can see the reason why. In our example, we set the secure source address for this port to 00-02-02-23-19-2a. The Last-Src-Addr clearly shows that at some point another machine tried to access our network through this port.

Console> (enable) **show port 12/19**

Port	*Name*	*Status*	*Vlan*	*Level*	*Duplex*	*Speed*	*Type*
12/19		*shutdown*	*1*	*normal*	*auto*	*auto*	*10/100BaseTX*

Port	*Security*	*Secure-Src-Addr*	*Last-Src-Addr*	*Shutdown*	*Trap*
12/19	*enabled*	*00-02-02-23-19-2a*	*00-01-02-23-1b-cf*	*Yes*	*enabled*

As with any good plan, there is a way to back out of the changes we have made on the switch. To enable the disabled port, enter the following command at the command prompt.

Console> (enable) **set port security 12/19 disable**
Port 12/19 port security disabled.

So far we have obtained detailed information from a host and have operated a switch to implement a port security policy. The following section will demonstrate how to effectively circumvent a port security enabled switch.

There are often legitimate reasons for wanting to change a machine's Mac address. For example, there may have been a manufacturing flaw and the same Mac may be burned onto multiple network interface cards on your network. In this case the option is usually to replace the NIC or configure the card to use a different Mac. As you will see, this feature will also help us to bypass network security that passes or restricts traffic based on a host's Mac address.

For this exercise, a machine running windows 2000 professional will be utilized. By following the proceeding steps, you will able to bypass port security.

1) From your windows 2000 desktop there should be an icon titled "My Network Places." Right click on the icon and select properties. The network and dial-up connections folder will open and in it you will see an icon titled "Local Area Connection."
2) Right click on the icon and select properties. The properties will be displayed and you will see your NIC at the top section with a configure button.
3) Select configure and click the advanced tab. There will be a property field displayed on the left.
4) Select the line that says network address.
5) After selecting the network address option you will see two options displayed on the right. Select the radio button that provides an option to enter a value. Enter the Mac address you would like to use as a single string. For example, in our scenario the port was restricted to using Mac address 00-02-02-23-19-2a. So, in this field we would enter 00020223192a.
6) Select ok and the host will begin using the Mac address you have just assigned to it. This will effectively bypass any port security settings that may be in effect on the port you are trying to access.

In conclusion, the security administrator should realize that many elements of a site security policy are easy to implement and just as easy to bypass. The challenge is to recognize and plan for these possibilities.

References:

- Microsoft, "NetBIOS Suffixes", http://support.microsoft.com/support/kb/articles/Q163/4/09.asp?LN=EN-US&SD=gn&FR=0, (July 12, 2000)

- Cisco Systems, Inc., "Managing your switches", http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35sa6/scg/kiconfig.htm#xtocid2727866, (July 12, 2000)

- Cisco Systems, Inc., "Cisco Network Monitoring and Event Correlation Guidelines", http://www.cisco.com/warp/public/cc/pd/wr2k/tech/cnm_rg.htm, (July 13, 2000)

- Microsoft, "How to troubleshoot duplicate media access control address conflicts", http://support.microsoft.com/support/kb/articles/Q164/9/03.asp?LN=EN-US&SD=gn&FR=0, (July 14, 2000)