CCNP Security Secure 642-637 Quick Reference

Andrew Mason

Cisco Press

CCNP Security Secure 642-637

Quick Reference

Andrew Mason

ciscopress.com

Table of Contents

Chapter 1
Cisco Layer 2 Security

A lot of attention is paid to securing the higher layers of the OSI reference model with network-level devices such as firewalls, intrusion protection systems (IPS), and applications such as antivirus and host-based intrusion protection (HIPS).

Layer 2 attacks occur, as you would expect, at Layer 2 of the OSI model. We know that switching operates at Layer 2; therefore, most of these attacks need to be mitigated in the switches you deploy in your network.

Layer 2 attacks are often overlooked when designing a network security solution; it is quite normal to find Layer 2 networks with no protection whatsoever. The availability of dedicated Layer 2 attack tools makes it necessary to defend against possible attack by implementing the features that Cisco offers within IOS Software.

One of the best tools used for testing Layer 2 security is Yersinia that is freely available from **http://www.yersinia.net/** and is part of the BackTrack 4 security distribution.

Types of Layer 2 Attacks

This section covers several types of Layer 2 attacks. This section also explains how to mitigate these attacks by implementing the correct control in Cisco IOS.

Following are the main types of Layer 2 attacks:

- CAM overflow
- VLAN hopping
- MAC spoofing
- Private VLAN attacks
- DHCP attacks

 Please see page 128 for more details.

CAM Overflow

Switches operate by building a reference table of MAC addresses and corresponding switch ports. Based on the destination MAC address, the switch knows which port to forward the frames to. This table is called the context-addressable memory (CAM) table.

The switch can hold only a specific number of MAC addresses in this table, depending on the resources available to the switch.

A CAM overflow attack occurs when an attacker connects to a single or multiple switch ports and then runs a tool that mimics the existence of thousands of random MAC addresses on those switch ports. The switch enters these into the CAM table, and eventually the CAM table fills to capacity. When a switch is in this state, no more new MAC addresses can be learned; therefore, the switch starts to flood any traffic from new hosts out of all ports on the switch.

A CAM overflow attack turns a switch into a hub, which enables the attacker to eavesdrop on a conversation and perform man-in-the-middle attacks.

Note
Dsniff can be downloaded from the authors website at http://monkey.org/~dugsong/dsniff/.

A common tool that performs CAM overflows is macof and is part of the Dsniff set of tools. This tool generates hundreds of thousands of random MAC addresses and floods these out onto the network. This is a useful tool for testing to see if your switch infrastructure is susceptible to CAM overflow attacks.

Cisco implemented a technology into IOS called Port Security that mitigates the risk of a Layer 2 CAM overflow attack.

Port Security

Port Security on a Cisco switch enables you to control how the switch port handles the learning and storing of MAC addresses on a per-interface basis. The main use of this command is to set a limit to the maximum number of concurrent MAC addresses that can be learned and allocated to the individual switch port.

If a machine starts broadcasting multiple MAC addresses in what appears to be a CAM overflow attack, the default action of Port Security is to shut down the switch interface; although, you can configure the switch just to discard any future Layer 2 frames received from the bogus MAC addresses.

 Please see page 128 for more details.

Note
Using a setting of 1 for the maximum allowed MAC addresses sounds good from a security point of view but might produce unwanted support overhead in all but the most locked-down environments.

Configuring Port Security

You must configure Port Security at the interface configuration level on a Cisco IOS switch. You need to allow Port Security on static access ports rather than dynamic access or trunk ports.

For illustrative purposes, this section shows a common Port Security configuration. You can configure Port Security to dynamically enable three MAC addresses on the configured port and make these connections sticky.

Start by ensuring that the switch port is a static access port:

```
Switch(config-if)# switchport mode access
```

The next step is to allow Port Security on the switch interface and to configure a maximum of three MAC addresses for the interface:

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
```

The switch learns the MAC addresses connected on the switch port and enables the first three it finds. In most cases, it is only a single end-user workstation connected to the switch and should see only a single MAC address. The switch needs to go through this process whenever you reboot the switch. You can allow the sticky mode for Port Security so that the MAC addresses that the switch learns about are stored when the configuration is saved so that they do not need to be relearned when the switch reboots. To allow sticky learning, enter the following command:

```
Switch(config-if)# switchport port-security mac-address sticky
```

You just reviewed a common configuration scenario in which the switch dynamically learns and remembers the MAC address of the devices connected to it. The other, and more secure, mechanism is to configure static Port Security by manually specifying the MAC address of the host connected to it.

If you have a switch port with the host MAC address 00:16:cb:96:95:94 connected to it, you can enter the following command to ensure that only this host can connect to the switch port:

 Please see page 128 for more details.

```
Switch(config-if)# switchport port-security mac-address 0016.cb96.9594
```

The default mode of port-security operation is to shutdown the port. There are three configurable modes of operation for port security - Shutdown, Restrict and Protect.

In the event that the switch port receives more MAC addresses than the configured maximum the port-security mode of operation dictates the action taken by the switch.

Shutdown. In the event that the switch port receives more MAC addresses than the configured maximum, the switch will shutdown the switch port. This is the default action mode.

Restrict. Restrict drops packets from unknown source MAC addresses received on the switch port and sends an SNMP Trap or a Syslog message to an administrator. The violation counter is also incremented.

Protect. Protect drops packets from unknown source MAC addresses. No SNMP Trap or Syslog message is generated and the violation counter is not incremented.

The following command is used to change the port-security mode of operation:

```
switchport port-security violation {shutdown | restrict | protect}
```

Note
When statically assigning MAC addresses, be careful of the possible support overhead that will be required for any moves or changes to the end-user infrastructure.

VLAN Hopping

Switches implement virtual LANs (VLAN). Users connect to access ports that are members of a VLAN as specified in the switch configuration. VLAN hopping is where a user can gain access to a VLAN not assigned to the switch port to which the user connects.

A user can achieve this in two ways against the default configuration of a Cisco switch port. The first and most commonly used VLAN hopping method is where the attacker makes his workstation act as a trunk port. Most switches, in the default

 Please see page 128 for more details.

configuration, need only one side of a connection to announce themselves as a trunk; then the switch automatically trunks all available VLANs over the switch port. This results in the attacker seeing all traffic across all VLANs.

The second way an attacker can hop VLANs is by using double tagging. With double tagging, the attacker inserts a second 802.1q tag in front of the existing 802.1q tag. This relies on the switch stripping off only the first 802.1q tag and leaving itself vulnerable to the second tag. This is not as common a method of VLAN hopping as using trunking.

To ensure you do not fall foul of a VLAN hopping attack, you must ensure that all your user ports are assigned as access mode ports. Any unused ports should be disabled and set as access mode ports by default.

To set a switch port to access mode, use the following configuration command from interface configuration mode:

```
Switch(config-if)# switchport mode access
```

By entering this command at the interface level, you switch the port into access mode; this port can never become a trunk port. It is a good practice to get into to ensure that all ports are configured in the correct mode. This should form part of your deployment strategy for all access layer switches in use within your organization.

When configuring a trunk port, the native VLAN need to be set to a unique VLAN, which is not routable or used elsewhere. To set a native VLAN on a trunk port, use the following configuration command from interface configuration mode:

```
Switch(config-if)# switchport trunk native vlan {number}
```

MAC Spoofing

MAC spoofing attacks are attacks launched by clients on a Layer 2 network. Attackers spoof their MAC address to perform a man-in-the-middle (MiTM) attack. In one common attack, the attacker pretends to be the default gateway and sends out a gratuitous Address Resolution Protocol (ARP) to the network so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway. An attacker on a fast enough host can capture and forward packets so that victims do not notice any change in their network access. Many tools available for download from the Internet, such as Ettercap, can accomplish such a task, and preventing such attacks is quite problematic.

 Please see page 128 for more details.

CCNP Security Secure 642-637 Quick Reference

Andrew Mason

Technical Editor: **Max Leitch**

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

First Printing December 2011

ISBN-10: 0-13-256645-1

ISBN-13: 978-0-13-256645-2

Warning and Disclaimer

This book is designed to provide information about the CCNP Security Secure exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is
implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc

Trademark Acknowledgments

All terms mentioned in this ebook that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this ebook should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical ebooks of the highest quality and value. Each ebook is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this ebook, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please be sure to include the ebook title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this ebook when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**