**CAM Table Overflow README**

**General Information**

* Author: Michael Ham
* Date: 1/15/2050
* Description: This is a presentation that covers the basics of Data Link layer concepts and issues along with a demonstration of the tool **macof** in Kali 2.0.

**Why You Should Care**

Hubs, Physical Layer devices, have been largely replaced by switches within a network. Despite the aging hardware and related limitations in hubs, one of he glaring issues with their continued use is security implications based upon how they handle traffic. All ports on a hub exist within the same collision domain and any traffic received on a port is forwarded out on al other ports. This may allow a listener on the network to uncover sensitive information such as usernames, passwords, insecure file transfers, etc.

Textbooks such as the CCNA Routing and Switching Study by Todd Lammle suggest that approximately 80% of internal network traffic should traverse a switched fabric. Switches have undoubtedly made a huge presence in almost every enterprise network. Switches make their forward/filter decisions partially based on the CAM table which maintains MAC address to physical port mappings. The CAM table allows switches to make intelligent forward/filter decisions so that non-broadcast traffic only gets sent to the intended destination. Due to hardware limitations, the CAM table may only hold a finite number of these types of mappings. The mappings stored within a CAM table typically have an expiration period which wall cause them to be removed if no traffic is received. Therefore, by maliciously filling the CAM table before entries expire, an attacker can cause the switch to fail open and operate like a hub.

**Three Main Ideas**

1. Switches are an integral part of enterprise and smaller networks that are suggested to handle 80% of network traffic.
2. Attackers may take an advantage of the Data Link Layer imperfections by filling a switches CAM table, causing it to fail open and operate like a hub. This may lead to disclosure of sensitive information.
3. The flaw exists within the specification itself, and therefore is not something that may be simply patched or easily solved. Vendors recommend implementing port security.

**Future Direction**

This topic could be further explored for determining the viability and vetting of defense mechanisms. Cisco recommends that users implement port security to defend against the CAM table overflows specifically. Furthermore, with the amount and type of traffic being generated, this type of attack should be detectable with standard monitoring tools. Can the attack be upgraded to make it more difficult to detect by the use and combination of another set of attacks such as VLAN hopping to expand the impact.

**Stream of Topics**

Additional topics related to this type of network-based attack may include some of the following:

* ARP and DNS poisoning
* Spanning Tree Protocol (SPT)
* MAC authentication attacks and spoofing
* VLAN Hopping

**Additional Resources**

* [Video Demonstration](https://youtu.be/sz4IyWFxo8o)
* [Black Hat - Hacking Layer 2: Fun with Ethernet Switches](http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf)
* [Cisco Background Info on CAM Overflows and Port Security](http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html#backinfo)
* [Cisco Show CAM Table](http://www.cisco.com/en/US/products/hw/switches/ps679/products_command_reference_chapter09186a00800d9f44.html#3338)
* [Hakipedia - CAM Table Overflow](http://hakipedia.com/index.php/CAM_Table_Overflow)