

Layer 2 Attacks and Mitigation Techniques for the Cisco Catalyst 6500 Series Switches Running Cisco IOS Software

MAC Address Overflow Attack and Mitigation Techniques

Authors:

Kevin Lauerman, CCSP, CISSP 80877 Jeff King, CCIE 11873, CCSP, CISSP 80875

Abstract

Security is at the forefront of most networks and many companies implement a comprehensive security policy encompassing many of the OSI layers, from application layer all the way down to IP security. However, one area that is often left untouched is hardening layer 2 and this can open the network to a variety of attacks and compromises.

This document will have a focus on understanding and preventing Layer 2 attacks on the Cisco® Catalyst® 6500 switching platform. Denial-of-Service (DoS) attacks are always a major concern. DoS attacks can come from internal and external sources. The focal point of this white paper will be to understand how a MAC Address Overflow Attack (DoS Attack) works and what techniques can be used on the Cisco Catalyst 6500 switch running Cisco IOS® Software to mitigate this type of attack. An attack tool called Ettercap was used to execute this attack.

A MacBook Pro and a Lenovo T61P was used for these test and acted as the attacker in some cases and the victim in others. Both computers ran VMware with different guest OSs acting as the attacker or victim.

Note that all the attacks performed in this document were done in a controlled lab environment. It is not recommended that you perform any of these attacks on your enterprise network.

Test Equipment

A Cisco Catalyst 6509E switch with a Supervisor 720-3B running Cisco IOS Software 12.2(33)SXI1 in an Advanced Enterprise Feature Set and a WS-X6748-GE-TX (10/100/1000) Ethernet line card was used. For the Attacker and Victim computers, an Apple MacBook Pro and a Lenovo T61P was used.

The MacBook Pro ran a native Mac OS X version 10.5.7 and also had VMware Fusion (2.0.5) with Ubuntu 9.04 and Windows XP SP2 virtual machines. The Lenovo T61P ran a Windows XP SP2 host OS and also had VMware with a Ubuntu 9.04 Virtual Machine.

WireShark was used for packet analysis in addition to using debugs on the Cisco Catalyst 6509E switch to show how the attack was unleashed and the response/actions of the switch.

MAC Address Overflow Attack

The intent of the MAC Address Overflow attack is for the attacker to be able to overrun the Cisco Catalyst 6509E switches Content-Addressable Memory (CAM) table. This will force packets for all new flows to be flooded out all ports, allowing the attacker to monitor (sniff) incoming packets.

The following hardware/software was used in the tests:

Victim 1:

- Hardware: Lenovo PC
- Software: Windows XP
- IP Address: 10.1.0.51/24
- MAC Address: 00:1c:25:1a:58:86
- NIC: Linksys USB300M (USB-to-Ethernet 10/100)
- Cisco Catalyst 6509E Port: GE 1/13

Victim 2:

- Hardware: MacBook Pro
- Software: Mac OS X 10.5.7 (and an FTP Client)
- IP Address: 10.1.0.61/24 (Static IP, excluded from the DHCP Server Pool of IP Addresses)
- MAC Address: 00:23:df:a0:cf:50
- NIC: Internal 10/100/1000 Ethernet
- Cisco Catalyst 6509E Port: GE 1/1

Victim 3:

- Hardware: Cisco Catalyst 6509E with a Supervisor 720-3B
- Software: Cisco IOS Software 12.2(33)SXI1
- IP Address: 10.1.0.1/24 (Interface VLAN 7)
- MAC Address: 00:d0:01:39:dc:00
- Line Card: WS-X6748-GE-TX (10/100/1000 Ethernet)

Attacker:

- Hardware: Apple MacBook Pro
- Software: Parent OS is OS X 10.5.7. Running Ubuntu 9.04 OS in VMware Fusion
- Attack Tool: Ettercap NG-0.7.3
- IP Address: 10.1.0.60/24 (Static IP, excluded from DHCP Server Pool of IP Addresses)
- MAC Address: 00:23:69:48:b8:9c
- NIC: Linksys USB300M (USB-to-Ethernet 10/100)
- Cisco Catalyst 6509E Port: GE 1/2

Steps for the MAC Address Overflow Attack:

- 1. Clear the MAC-Address-Table (CAM) before running the attack
- 2. Ping the switch (Interface VLAN 7 = 10.1.0.1)
- 3. View MAC-address-table ("show mac-address-table")
- 4. Edit the Ettercap Configuration File ("etter.conf")
- 5. Open Ettercap attack tool inside Ubuntu OS
 - a. Select "Promisc Mode" (Promiscuous)
 - b. Select the interface to use (eth2 in our case)
 - c. Scan for Hosts on the Subnet

- d. View the Hosts List
- e. Start Sniffing
- f. View Connections (should be blank at this point)
- g. Start Random MAC Address Flooding Attack ("rand_flood" plugin)
- 6. Run Network Analyzer on Attacker to View Gratuitous ARPs to switch
- 7. View MAC Address Count (used/available) in CAM Table of switch
- 8. View MAC Address (CAM) Table
- 9. View FTP Client (MacBook Pro Victim) session
- 10. View Connections in Ettercap (10.1.0.61 to 10.1.0.51) for FTP
- 11. Kill Active FTP Connection between Victims
- 12. Mitigation for the MAC Address Overflow Attack
- 13. Summary

Figure 1 shows a diagram of the components used in the MAC Address Overflow Attack test. Note that the MacBook Pro (Victim) was connected to the Cisco Catalyst 6509E switch via the integrated 10/100/1000 Ethernet port ,and the Ubuntu Virtual Machine (running in VMware Fusion on the MacBook Pro) had a dedicated external Linksys USB300M 10/100 (USB-to-Ethernet) Network Adapter. Each was independent and no NAT or Bridging was being used between the host OS (OS X 10.5.7) and the Virtual Machine (Ubuntu 9.04).

Figure 1.



Before the MAC Address Overflow attack was started, a few configuration tasks were completed. Clearing out the dynamic MAC Address-Table on the Cisco Catalyst 6509E switch was performed first. This was done using the "clear mac address-table dynamic" command on the switch. Figure 2 shows this output and also displays the ARP cache.

Figure 2.

③ telnet	8	bash	0	bash	0	bash	8	bash	>
6509E#clear m address interface vlan <cr></cr>	ac addres address k interface vlan keyw	s-table dyn eyword keyword ord	amic	2					
6509E#clear m MAC entries c	ac addres leared.	s-table dyn	amic						
6509E#show ma address interface module vlan <cr></cr>	c address address k interface display e VLAN keyw Dutput mo	-table dyna eyword keyword ntries in D ord difiers	umic ? IFCcar	d					
6589E#show ma Legend: * - p age - n/a - vlan mac	c address rimary en seconds not avai address	-table dyna try since last lable tupe	umic seen learn	aae			ports		
 * 255 ААНА	 93e2 дЮО	-++ dunamic	Vae	++	615				
* 7 001c.	251a.5886	dynamic	Yes		611	/13			
* 7 0023.	dta0.ct50	dynamic	Yes	i e	Gi1	/1			
* 7 0023. 6509E#show_ar	dta0.ct50 p	dynamic	Yes	Li	Gil	/1			

Next, using the Network Tools GUI on the Ubuntu 9.04 Virtual Machine, switch connectivity was verified by using ping (10.1.0.1 = Interface VLAN 7 on the Cisco Catalyst 6509E).

Figure 3.

evices Ping	Netstat	Traceroute	Port Scan	Lookup	Finger	Whois	
<u>N</u> etwork add	ress: 10.	1.0.1					
Send:	۰	only 5	requests	O Unli	mited re	quests	
						Pir	ng
Round Trip	Time Sta	atistics Tr	ansmissio	n Statis	tics		
Minimum:	1.17 ms	S I	Packets tra	nsmitted	: 5		
Minimum: Average:	1.17 ms 4.89 ms	5 5	Packets tra Packets rec	nsmitted eived:	: 5 5		
Minimum: Average: Maximum:	1.17 ms 4.89 ms 11.60 ms	5 5 5	Packets tra Packets rec Successful	nsmitted eived: packets:	: 5 5 100%		
Minimum: Average: Maximum:	1.17 ms 4.89 ms 11.60 ms	5	Packets tra Packets rec Successful	nsmitted æived: packets:	: 5 5 100%		
Minimum: Average: Maximum: Time (ms):	1.17 ms 4.89 ms 11.60 ms 11.60	1.54	Packets tra Packets rec Successful 1.17	nsmitted eived: packets:	: 5 5 100%	2.07	7

Figure 4 shows a snapshot of the current MAC Address Table on the Cisco Catalyst 6509E switch before the MAC Address flooding attack was started. Note that there are two very similar show commands. There is the "**show mac** address-table dynamic" and the "**show mac-address-table**." Both show the same information.

Figure 4.

C) te	elnet 🛞	bash	8	bash	🕲 bash	🙁 bash
65	09E#s	how mac-address	-table				
Le	gend:	* - primary er	itry				
		age - seconds	since last	seen			
		n/a - not avai	lable				
	vlan	mac address	type	learn	age	port	8
*	255	00d0.03e2.a000) dynamic	Yes	5	615/2	
*		0000.0000.0000	l static	No		Router	
*	255	3333.0000.0000	l static	Yes		Gi1/1,Gi1/2,G	i1/13,Gi1/14
						Gi5/2,Router,	Switch
*	255	3333.0000.0001	static	Yes		Switch	
*	7	001c.251a.5886	o dynamic	Yes	8	611/13	
*	7	0023.6924.c38c	dynamic	Yes	60	Gi1/14	
*	7	0023.6948.6890	: dynamic	Yes	20	611/2	
*		0000.0000.aaaa	ı static	No		Switch	
*	255	3333.0000.0016	i static	Yes		Switch	
*	7	000f.f86d.d800	l static	No		Router	
*	7	0023.dfa0.cf50	l dynamic	Yes	0	611/1	
*	50	3333.0000.0000	l static	Yes		Gi1/1,Gi1/2,G	i1/13,6i1/14
						Gi5/2, Router,	Switch
*	1	3333.0000.0000	l static	Yes		Gi1/1,Gi1/2,G	i1/13,6i1/14
						Gi5/2, Router,	Switch
*	7	3333.0000.0000	l static	Yes		Gi1/1,Gi1/2,G	i1/13,6i1/14
						Gi5/2, Router,	Switch
*	10	3333.0000.0000	l static	Yes	E (=)	Gi1/1,Gi1/2,G	i1/13,6i1/14
						Gi5/2, Router,	Switch
*	20	3333.0000.0000	l static	Yes		Gi1/1,Gi1/2,G	i1/13,6i1/14
						Gi5/2,Router,	Switch
*	20	3333.0000.0001	static	Yes		Switch	
*	10	3333.0000.0001	static	Yes		Switch	
*	1	3333.0000.0001	static	Yes		Switch	
*	7	3333.0000.0001	static	Yes		Switch	
*	50	3333.0000.0001	static	Yes		Switch	
*	255	000f.f86d.d800	l static	No		Router	
*	20	3333.0000.0016) static	Yes		Switch	
*	10	3333.0000.0016	i static	Yes		Switch	
*	7	3333.0000.0016) static	Yes		Switch	
*	. 1	3333.0000.0016	static	Yes		Switch	
*	50	3333.0000.0016) static	Yes		Switch	

Figure 5 is a screen shot of the Cisco Catalyst 6509E console after clearing the ARP table and MAC Address table. The two hosts (10.1.0.61 – MacBook Pro running OS X 10.5.7 and 10.1.0.51 – Lenovo T61P running Windows XP) Ethernet are disconnected from the switch and then reconnected. Figure 5.

6509E# 6509E#sho	arp					
Protocol	Address	Age	(min)	Hardware Addr	Туре	Interface
Internet	10.1.0.1			000f.f86d.d800	ARPA	Vlan7
Internet	10.1.0.60		Θ	0023.6948.b89c	ARPA	Vlan7
Internet	10.1.0.50		Θ	0023.6924.c38c	ARPA	Vlan7
Internet	172.18.176.153		0	00d0.03e2.a000	ARPA	Vlan255
Internet	172.18.176.198			000f.f86d.d800	ARPA	Vlan255
6509E#						

Ettercap Configuration (etter.conf) File Modifications

Note that some modifications were required to be made to the "etter.conf" file on the Ubuntu (Virtual Machine). One of the default settings in the etter.conf file (located in the /etc folder in Ubuntu 9.04) was changed. Also the "**port_steal_send_delay**" was modified from the default value of "2,000" to a value of "1." Below is the screen shot of this action. This modification was required in order to be able to generate enough traffic to overflow the switch's CAM table.

Figure 6.

etter.conf (/	(etc) - gedit	
<u>File Edit View Search Tools</u>	Documents Help	
New Open Save Print	Undo Redo Cut Copy	Paste ¥
<pre>[mitm] arp_storm_delay = 10 arp_poison_warm_up = 1 arp_poison_delay = 10 arp_poison_icmp = 1 arp_poison_reply = 1 arp_poison_request = 0 arp_poison_equal_mac = 1 dhcp_lease_time = 1800 port_steal_delay = 10 port_steal_send_delay = 1</pre>	<pre># milliseconds # seconds # seconds # boolean # boolean # boolean # boolean # seconds # milliseconds # microseconds</pre>	

Running the Ettercap Attack Tool

The Ettercap attack tool GUI was opened and "**Promiscuous Mode**" was selected on the Ubuntu Virtual Machine interface (eth2 in our case).

1. Select Promiscuous Mode

Figure 7.

	ettercap NG-0.7.3	
<u>File</u> Sniff	Options Help	
	□ Unoffensive ☑ Promisc mode Set netmask N	

2. Select Interface

Figure 8.

	ettercap NG-0.7.3	- D X
<u>File</u> Sniff	Options <u>H</u> elp	
	ettercap input 🛛	
	Network interface : eth2 Image: Cancel	
	SERCAR	

3. Scan for Host on the subnet

Figure 9.



4. View the Host List

Figure 10.

			e	iterca	NG-0.	7.3			
Start	Targets	<u>H</u> osts	View	<u>M</u> itm	Filters	Logging	Plugins	<u>H</u> elp	
		Hos Hos	ts list) I	H			
		Sca	n for ho	sts	Ctrl+	S			
		🖻 Loa	d from	file	Ctrl+(c			
		🔮 Sav	e to file		Ctrl+	S			

Output from Step 4

Figure 11.

		e	tercap	NG-0.	7.3			
Start Targe	ets <u>H</u> osts	View	Mitm	<u>Filters</u>	Logging	Plugins	<u>H</u> elp	
Host List 💥								
IP Address	MAC Addr	ess	Desc	ription				
10.1.0.1	00:0F:F8:6	D:D8:0	D					
10.1.0.50	00:23:69:2	4:C3:80	5					
10.1.0.51	00:1C:25:1	LA:58:80	5					
10.1.0.61	00:23:DF:A	40:CF:50)					

5. Start Sniffing (monitoring) mode

Figure 12.

			e	itercap) NG-0.	7.3			
<u>S</u> tart	Targets	<u>H</u> osts	View	Mitm	<u>F</u> ilters	Logging	Plugins	<u>H</u> elp	
😑 Sta	art sniffing	j Ct	rl+W						
🔴 Sto	op sniffing	C	trl+E						
€ <u></u> E <u>x</u>	it	C	trl+X						
52 00	rts monit	arad			100000000000000000000000000000000000000				
7587 n	nac vendo	or finger	print						
1698 to 2183 k	cp OS fing nown sen	erprint vices							
Rando	mizing 25	5 hosts	for scal	nning	oste				
4 hosts	added to	the hos	sts list.		0515				=

6. View Connections. Note that no "Targets" were specified.

Figure 13.

			et	tercap	NG-0.	7.3			
Start	Targets	Hosts	View	Mitm	<u>H</u> elp				
				nnection			Shift+C		
			Pro	files		:	Shift+O		
			🛃 <u>S</u> ta	tistics			S		
			✓ Res	olve IP	address	es			
			₩ <u>V</u> is	ualizati	on meth	od	v		
			Vis	u <mark>aliz</mark> ati	on <u>r</u> ege>	(R		
			🙀 Set	the <u>W</u> E	P key		w		

Initiate Ettercap "rand_flood" MAC Address Flooding Attack

Next the "rand_flood" attack plugin in Ettercap was run . That flooded the CAM Table on the Cisco Catalyst 6509E with random MAC Addresses. Once the MAC address table on the switch was exhausted of the available MAC Address space, Ettercap was setup in sniffing mode to see if the FTP session from host 10.1.0.61 (MacBook Pro) to host 10.1.0.51 (Windows XP – Lenovo T61P) would work.

7. Start the Random MAC Address Flooding Plugin

The snapshots below show the Gratuitous ARPs being sent out by Ettercap to the Cisco Catalyst 6509E switch.

Figure 14.

Start Targets Hosts View Mitm Eilters Logging Plugins Help Connections ≈ Plugins ≈ Name Version Info
Connections # Plugins #
Name Version Info
link_type 1.0 Check the link type (hub/switch)
pptp_chapms1 1.0 PPTP: Forces chapms-v1 from chapms-v2
pptp_clear 1.0 PPTP: Tries to force cleartext tunnel
pptp_pap 1.0 PPTP: Forces PAP authentication
pptp_reneg 1.0 PPTP: Forces tunnel re-negotiation
* rand_flood 1.0 Flood the LAN with random MAC addresses
remote_browser 1.2 Sends visited URLs to the browser
reply_arp 1.0 Simple arp responder
repoison_arp 1.0 Repoison after broadcast ARP
scan_poisoner 1.0 Actively search other poisoners
search_promisc 1.2 Search promisc NICs in the LAN
emb clear 1.0 Tries to force SMR cleartext auth
39 protocol dissectors
53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint 2183 known services
Randomizing 255 hosts for scanning
Scanning the whole netmask for 255 hosts

Starting Unified sniffing...

Activating rand_flood plugin... rand_flood: Start flooding the LAN...

8. Run Network Analyzer to Capture Gratuitous ARPs to 6509E Switch

Figure 15.

	eth2: Cap	turing - Wireshark		
<u>File Edit View Go Cap</u>	oture <u>Analyze</u> <u>Statistics</u> <u>H</u> elp			
				~
Eilter:		← Expression	🔮 Clear 🎻 Apply	
No. Time Source	Destination	Protocol Info		^
197410 0.002281 d7:c1:	:b3:1d:2d: 0f:b5:bf:12:45:ca	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197411 0.002293 f9:08:	:c7:4f:d4: 4c:19:20:62:8c:d	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197412 0.002386 d9:4b:	:bd:2c:3f: 9f:19:95:7c:c5:38	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197413 0.002385 20:aa:	:b6:24:89: d2:4a:f0:1c:90:b1	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197414 0.002325 68:c7:	:b5:3c:85: 52:85:ad:2e:82:2e	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197415 0.002296 8c:6e:	:a2:6c:2e: 8e:ab:7c:48:b1:34	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197416 0.002295 ee:13:	:03:18:ea: bb:60:95:29:4c:b	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197417 0.002314 2b:6e:	:81:3c:b1: ac:fb:de:51:02:30	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197418 0.002397 de:e4:	:ee:42:bb: 48:fa:6e:03:d7:eo	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197419 0.002369 8f:ad:	:4e:44:94: 63:c3:dd:03:69:f9	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197839 0.002161 a0:3b:	:0d:49:61: b6:45:40:63:f9:3a	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197840 0.002805 3f:9a:	:9e:07:0f: 41:1f:be:1c:cc:60	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	
197841 0.002717 8c:80:	:d1:07:fe: 0c:b7:8a:28:84:48	ARP Gratuitous A	ARP for 0.0.0.0 (Request)	

Next, Wireshark was run on the attacker machine (Ubuntu 9.04 Virtual Machine) that was also running the Ettercap attack tool GUI. After running the MAC Address Overflow attack (Ettercap "rand_flood" attack), it can be seen that all of the MAC Addresses in the Cisco Catalyst 6509E Content Addressable Memory (CAM) Table (Figure 16) were exhausted. Note that the Cisco Catalyst 6509E has a Supervisor 720-3B and is running 12.2(33)SXI1 Cisco IOS Software.

9. View Count of Available/Used MAC Address in CAM Table

Figure 16.



Figure 17 shows the first page (of many) listing the random MAC Addresses flooded in the Cisco Catalyst 6509E's MAC Address Table from the Ubuntu Attacker machine running Ettercap's "rand_flood" plugin.

10. MAC-Address-Table Listing (just first page)

Figure 17.

: 	الم مراجع الم							^
65 Le	09E#s gend :	how mac address-1 * - primary ent age - seconds si n/a - not availa	table ry ince last able	seen				8
	vlan +	mac address	type	learn	age		ports	
**	7	f27e 9679 038d	dynamic	Vec	1120	611/2		
¥	4	h875 907c 4480	dynamic	Vec	1120	Gi1/2		
*	4	bofd fb4a coec	dynamic	Yes	1120	Gi1/2		
*	7	fedc 8f6f 7888	dynamic	Yes	1120	Gi1/2		
¥	7	f271, 1738, db59	dynamic	Yes	1115	Gi1/2		
*	7	aa38,204c,d3f7	dynamic	Yes	1110	Gi1/2		
*	7	c627.f87a.57d5	dynamic	Yes	1105	Gi1/2		
*	7	4432.4415.293f	dynamic	Yes	1100	Gi1/2		
ŧ	7	d8b5.021c.bcda	dynamic	Yes	1095	Gi1/2		
*	7	06d3.9265.aaca	dynamic	Yes	1095	Gi1/2		
ŧ	7	0480.8839.belc	dynamic	Yes	1090	Gi1/2		
ŧ	7	c4b0.ec12.f1df	dynamic	Yes	1090	Gi1/2		
*	7	c82f.237b.5933	dynamic	Yes	1085	Gi1/2		
*	7	e4d6.8144.4921	dynamic	Yes	1085	Gi1/2		
*	7	26a7.623b.8ff0	dynamic	Yes	1085	Gi1/2		
*	7	2e1e.9314.5afd	dynamic	Yes	1085	Gi1/2		
*	7	8a91.f242.da51	dynamic	Yes	1125	Gi1/2		
*	7	0e9c.1a56.8f83	dynamic	Yes	1115	Gi1/2		
ŧ	7	1cbb.7004.1039	dynamic	Yes	1115	Gi1/2		
*	7	b664.f622.605e	dynamic	Yes	1115	Gi1/2		
*	7	aaff.cb41.d2da	dynamic	Yes	1110	Gi1/2		
*	7	32d3.915f.7a67	dynamic	Yes	1110	Gi1/2		
*	7	9e71_8134_5dd3	dynamic	Yes	1110	Gi1/2		U

In Ettercap on the attacker's machine the "**sniffing**" window was viewed while getting ready to open up an FTP session from the FTP Client (10.1.0.61 – MacBook Pro) to the FTP Server (10.1.0.51 – Lenovo T61P). Keep in mind that the Ettercap "**rand_flood**" plugin was still running and that all 65,536 available MAC Addresses had been consumed on the Cisco Catalyst 6509E.

Figure 18.

2		10.1.0.5	1 - F	leZilla	6	
<u>File Edit View</u>	<u>Transfer</u> Server	Bookmarks Help				
💼 📰 🌬	tr Q 🖸 🎐 C	🖉 R 📑 🖽 👓				
Host: 10.1.0.51	<u>U</u> sername:	anonymou: Pass <u>w</u> ord:		Port: Quickconnect		
Response: 227 f Command: LIST Response: 125 l Response: 226 c Status: Direct	Entering passive mod Using existing data c Closing data connect ctory listing successf	de (10,1,0,51,4,119) onnection ion ul				< III >
Local site: /med P nome D 1 lib 1 lost+fo P media	lia/ bund			Remote site: /		`
Filename	Filesize Filety	be Last modified		Filename	Filesize Filetype	Last
cdrom cdrom0 cdrom1	Directo Directo Directo	ory 05/14/2009 04: ory 05/14/2009 04: ory 05/14/2009 04:	() m	 □ 	21,839, Unknown	06/2:
floppy	Directo	ory 05/14/2009 04:	~	1 file. Total cize: 21 920 140 huter		>
I file and 5 direc	tories. Iotal size: 0 t	ytes		1 me. lotal size: 21,039,140 bytes		
Server/Local file	Direction	Remote file		Size Priority Status		
Queued files	Failed transfers	Successful transfers	J			
				2 []2	Queue: empty	• •

Snapshot of MacBook Pro (Victim 2) with an FTP session to Lenovo Windows XP (Victim 1)

The following shows the connections that showed up in Ettercap for Victim 2 (10.1.0.61 – MacBook Pro). The connections screen was dynamic, and one can see the "**state**" of the connection change from active, to idle, to closed.

11. View Connections in Ettercap

Figure 19.

				e	itercap) NG-0.	7.3			
<u>S</u> t	art <u>T</u> arge	ts <u>H</u> os	sts	View	Mitm	<u>F</u>ilters	Logging	Plugins	<u>H</u> elp	
H	ost List 🕿 Name	Plugir	is ≱ Ve	Pro	nnectio ofiles	ns		Shift+C Shift+O		
	isolate link_type pptp_chap pptp_clea	oms1 r	1.0 1.0 1.0 1.0	 ✓ Res W Vis W Vis 	solve IP sualizati sualizat	address ion meth ion <u>r</u> ege	ses nod x	V R	ıms-v2	
*	pptp_pap pptp_rene rand_flood remote_b reply_arp repoison_ scan_pois search_pr smb_clea smb_dow stp_mang	eg rowser arp oner omisc r n ler	1.0 1.0 1.2 1.0 1.0 1.0 1.0 1.0 1.0 1.0	<u></u>	t the <u>W</u> PPTP: Fe Flood th Sends v Simple & Repoiso Actively Search p Tries to Become	EP key prces tur ne LAN w isited UI arp resp n after b v search promisc force SM force SM e root of	nnel re-neg vith randor RLs to the onder oroadcast v other pois NICs in the IB clearte IB to not u a switches	W gotiation m MAC a browser ARP oners e LAN xt auth use NTLM s spannir	ddresses 12 key auth 19 tree	1
Ran Sca 2 h Act ran Sta	ndomizing nning the osts added ivating ran d_flood: St rting Unifie	255 ho whole r I to the id_flood art floo ed sniff	sts f hetn hos d plu ding ing	for sca nask fo ts list. Igin g the L	nning or 255 h AN	osts				

Undetected by the two Victim machines engaged in the FTP session, Ettercap was able to capture the username and password.

Figure 20.

D				et	terca	рÑ	G-0.7	.3			
Sta	art <u>T</u> arge	ts <u>H</u> os	sts	View	Mitm	Ē	Iters	Logging	Plugins	<u>H</u> elp	
Plu	ugins 🕿	Connec	tio	ns 🛪							
	Host	Port		Host	Po	ort	Proto	State	Bytes		
	10.1.0.60	631	-	10.1.0.2	255 63	31	U	active	1604		
	10.1.0.51	137	-	10.1.0.2	255 13	37	U	idle	900		
	10.1.0.60	34492	-	10.1.0.1	1 23	3	Т	idle	1557		
*	10.1.0.61	49964	- 23	10.1.0.5	51 21	l,	Т	idle	527		
	10.1.0.61	49965	-	10.1.0.5	51 18	316	Т	closed	276		
	10.1.0.61	49966	-	10.1.0.5	51 18	317	Т	closed	276		
	View	Details			<u>K</u> il		onnecti	on	Expur	nge Conne	ections
Sca 4 ho	nning the osts added	whole r	net ho	mask fo sts list	r 255 l	nost	S				^

12. Combined View of Active Connection (FTP session)

Figure 21.

		ettercap	NG-0.	7.3			
<u>Start</u> Targe	ts <u>H</u> osts <u>V</u>	iew <u>M</u> itm	<u>F</u> ilters	Logging	Plugins	Help	
Host List 📾	Plugins #	Connection	s 🕫 🖸	onnection o	data 🛪		
10.1.0.61:49 220 3Com 3 USER anony 331 User n	934-10.1.0. CDaemon FTF mous. ame ok, nee	51:21 9 Server Ve ed password	ersion 1.	2.0.			
230 User l SYST. 215 UNIX T FEAT.	ogged in. ype: L8.						≡.
MDTM. SIZE. REST STREA 211 End.	M.						
PWD. 257 "/" is TYPE I. 200 Type s	current di	irectory.					
PASV. 227 Enteri	ng passive	mode (10,	L,0,51,	14,208).			
	Split View	i .			Kill Conne	ection	
Scanning the 2 hosts added	whole netma	sk for 255 h list	osts				

2 hosts added to the hosts list... Activating rand_flood plugin... rand_flood: Start flooding the LAN... Starting Unified sniffing...



Besides being able to see the FTP session from both Victims' viewpoints (including username/password/file listings/etc), the FTP connection could also be killed from within Ettercap.

13. Kill the FTP Connection Between Victim Machines

Figure 22.

		ettercap	NG	-0.7.3				_ 0	X
Start Target	ts <u>H</u> osts <u>N</u>	<u>/</u> iew <u>M</u> itm	<u>F</u> ilte	ers <u>L</u> ogg	ging	Plugins	<u>H</u> elp		
Host List 🛚	Plugins #	Connection	s 🛛	Connect	ion d	ata 🕺			
10.1.0.61:499	934			10.1.0.51	:21				
TYPE I. NOOP. NOOP. PWD. PWD. PWD. PASV. LIST. PASV				200 Com 257 "/" 227 Ent 1,0,51, 125 Usin tion. 226 Clo 227 Ent 1,0,51, 125 Usin	mand is erind 16,2 ng e: sing erind 16,2 ng e:	OK. current g passi 7). xisting data c g passi 8). xisting	direct ve mode data d connecti ve mode data d	connec connec con. e (10, connec	
LIST -a. PWD. CDUP. PWD. TYPE I. NOOP. NOOP.		Th	ie co	nnection	was I	killed !!	nnecti direct cessfu direct	ion. cory. il. cory.	< III
Join Vie	ws	Inject Data		Inje	ct <u>F</u> il	e	<u>K</u> ill Co	nnection	Ĭ

Mitigation for the MAC Address Overflow Attack

There are a number of actions that can be configured on the Cisco Catalyst 6500 Series Switch to handle mitigation for this type of attack. Each of these mitigation techniques is reviewed in the following section. Take a look at the snapshot below from the Cisco Catalyst 6509E switch.

Figure 23.

6509E#config t	
Enter configura	tion commands, one per line. End with CNTL/Z.
6509E(config)#m	ac-address-table ?
aging-time	Set MAC address table entry maximum age
aging-type	Enable routed MAC entries aging
learning	Enable a MAC table learning feature
limit	Enter parameters for mac limit feature
notification	Enable a Notification feature
static	static keyword
synchronize	Synchronize MAC address table entries in the system

The first mitigation feature that is discussed is the "mac-address-table limit" command and its related parameters.

Figure 24.

6509E(config)#m	ac-address-table limit ?	
action	Enter action	
interface	interface	
maximum	Enter max allowed entries	
notification	Enter type of Notification	
vlan	vlan number for mac limit	feature
<cr></cr>		

The mitigation is started by limiting the number of MAC addresses that can be received on each of the access layer switch ports on the Cisco Catalyst 6509E. Since it is known that the attacker machine was running Ettercap ("rand_flood") and was connected to GE1/2 on the switch, the global command "**mac-address-table limit interface** gi1/2 maximum 15 action limit" was added. This command limits the number of accepted MAC addresses inbound on port GE1/2 to 15.

Figure 25.



Note the other two configurable options are "warning" and "shutdown."

In the snapshot below, it can be seen that GE 1/2 (Attacker machine) reached its maximum limit of (15) MAC address entries. The switch enforced this limit and did not accept any more MAC addresses on the input interface GE 1/2.

Figure 26.



It can also be seen that the system messages caught in the logging buffer on the switch indicated that port GE 1/2 reached the maximum limit (15 in our case) configured.

Figure 27.



Another mitigation technique that is effective for the MAC Address Overflow attack is the **DHCP Snooping** and **Dynamic ARP Inspection (DAI)** combination. These mitigation features are also very effective for the ARP Poisoning (Man-In-The-Middle [MITM]) and DHCP Consumption attacks. The Cisco Catalyst 6509E switch is configured for DHCP Snooping and DAI using the following commands. Note that **DHCP Snooping is required** in order to be able to configure and use the Dynamic ARP Inspection (DAI) feature.

Figure 28.

```
6509EWconfig t
Enter configuration commands, one per line. End with CNTL/Z.
6509E(config)#ip dhep snooping vlan 7
6509E(config)#ip dhep snooping vlan 7
6509E(config)#ip arp inspection vlan 7
6509E(config)#ip arp inspection log-buffer entries 1024
6509E(config)#ip arp inspection log-buffer logs 1024 interval 10
6509E(config)#ip arp inspection log-buffer logs 1024 interval 10
6509E(config)#ip arp inspection log-buffer logs 1024 interval 10
6509E(config)#ip arp inspection torst
6509E(config)#ip arp inspection trust
6509E(config-if)#ip dhep snooping trust
6509E(config-if)#ip arp inspection trust
6509E(config-if)#ip arp inspection trust
6509E(config-if)#ip dhep snooping trust
6509E(config-if)#ip arp inspection trust
6509E(config-if)#ip dhep snooping trust
6509E(config-if)#ip arp inspection trust
```

With the above commands enabled on the switch, the MAC Address Overflow attack is stopped. Prior to enabling DHCP Snooping and DAI, the Ettercap "**rand_flood**" attack exhausted all 65,536 available MAC Addresses in the CAM table. With these mitigation features enabled, here is what was seen.

Figure 29.



Notice the large difference between the number of available MAC addresses and the number of MAC Addresses In Use.

Note that for this test, because a static IP address was used on the attacker machine (10.1.0.60/24), a static DHCP binding was added in the switch configuration to bind the MAC address and IP address of the attacker machine to interface GE 1/2 on the switch. If this was not done, then the last two mitigation features configured would put the switch port out of service. Here is the format of the command.

Figure 30.

6509E#config t Enter configuration commands, one per line. End with CNTL/Z. 6509E(config)#ip source binding 0023.6948.b89c vlan 7 10.1.0.60 interface gi 1// 6509E(config)#end cronc#

Summary

The **MAC Address Overflow attack** is effective if the proper mitigation techniques are not in place on the Cisco Catalyst 6500 series switch. By using publicly (free) and available Layer 2 attack tools found on the Internet, anyone who understands how to setup and run these tools could potentially launch an attack on your network.

MAC address monitoring is a feature present on Cisco Catalyst 6500 Series switches. This feature helps mitigate MAC address flooding and other CAM overflow attacks by limiting the total number of MAC addresses learned by the switch on per-port or per-VLAN basis. With MAC Address Monitoring, a maximum threshold for the total number of MAC addresses can be configured and enforced on a per-port and/or per-VLAN basis. MAC address monitoring in Cisco IOS Software allows the definition of a single upper (maximum) threshold. In addition, the number of MAC addresses learned can only be monitored on a per-port or per-VLAN basis, and not a per-port-per-VLAN. By default, MAC address monitoring is disabled in Cisco IOS Software. However, the maximum threshold for all ports and VLANs is configured to 500 MAC address entries, and when the threshold is exceeded the system is set to generate a system message along with a syslog trap. These default values take effect only when MAC address monitoring is enabled. The system can be configured to notify or disable the port or VLAN every time the number of learned MAC addresses exceeds the predefined threshold. In our test, we used the "mac-address-table limit" command on the access layer port interface to configure the MAC address monitoring feature.

Two other Cisco IOS Software features that can be used to mitigate the MAC Address Overflow attack include **DHCP Snooping** coupled with **Dynamic ARP Inspection (DAI)**. By using the DHCP Snooping and Dynamic ARP Inspection (DAI) features, we are able to stop multiple types of Layer 2 attacks.

DHCP Snooping is a security feature capable of intercepting DHCP messages crossing a switch and blocking bogus DHCP offers. DHCP Snooping uses the concept of trusted and untrusted ports. Typically, the trusted ports are used to reach DHCP servers or relay agents, while untrusted ports are used to connect to clients. All DHCP messages are allowed on trusted ports, while only DHCP client messages are accepted on untrusted ports. As neither servers nor relay agents are supposed to connect to untrusted ports, server messages like DHCPOFFER, DHCPACK, and DHCPNAK are dropped on untrusted ports. In addition, DHCP Snooping builds and maintains a MAC-to-IP binding table that is used to validate DHCP packets received from untrusted ports. DHCP Snooping discards all untrusted DHCP packets not consistent with the information in the binding table. For DHCP snooping binding table contains the MAC address, IP address, lease time in seconds, and VLAN port information for the DHCP clients on the untrusted ports of a switch. The information that is contained in a DHCP-snooping binding table is removed from the binding table when its lease expires or DHCP Snooping is disabled in the VLAN.

Dynamic ARP Inspection (DAI) is a security feature that helps prevent ARP poisoning and other ARP-based attacks by intercepting all ARP requests and responses, and by verifying their authenticity before updating the switch's local ARP cache or forwarding the packets to the intended destinations. The DAI verification consists primarily of intercepting each ARP packet and comparing its MAC address and IP address information against the

MAC-IP bindings contained in a trusted binding table. DAI discards any ARP packets that are inconsistent with the information contained in the binding table. The trusted binding table is dynamically populated by DHCP snooping when this feature is enabled. In addition, DAI allows the configuration of static ARP ACLs to support systems that use statically configured IP addresses and that do not rely on DHCP. DAI can also be configured to drop ARP packets with invalid IP addresses, such as 0.0.0.0 or 255.255.255.255.255, and ARP packets containing MAC addresses in their payloads that do not match the addresses specified the Ethernet headers.

Another important feature of DAI is that it implements a configurable rate-limit function that controls the number of incoming ARP packets. This function is particularly important because all validation checks are performed by the CPU, and without a rate-limiter, there could be a DoS condition.

DAI associates a trust state with each interface on the system, similar to DHCP Snooping. Packets arriving on trusted interfaces bypass all DAI validation checks, while those arriving on untrusted interfaces go through the DAI validation process. In a typical network configuration for DAI, all ports connected to host ports are configured as untrusted, while all ports connected to switches are configured as trusted. With this configuration, all ARP packets entering the network from a given switch will have passed the security check. By default, DAI is disabled on all VLANs, and all ports are configured as untrusted.

As discussed earlier, DAI populates its database of valid MAC address to IP address bindings through DHCP snooping. It also validates ARP packets against statically configured ARP ACLs. It is important to note that ARP ACLs have precedence over entries in the DHCP snooping database. ARP packets are first compared to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, then the packet will be denied even if a valid binding exists in the database populated by DHCP snooping.

Note that configuring DHCP Snooping is a prerequisite to configure Dynamic ARP Inspection (DAI). It is also worth noting that if you plan to use any static IP addresses are planned to be used when configuring DHCP Snooping and DAI, a static IP-to-MAC address mapping must also be entered in your Cisco Catalyst 6500 switches configuration. For instance, lets say that we want to assign a static IP-to-MAC mapping for the IP address 10.1.0.60 with the MAC address of 0023.6948.B89C for interface GE1/2 on VLAN 7 is required. The global configuration command on switch would be:

ip source binding 0023.6948.B89C vlan 7 10.1.0.60 interface Gi1/2

References

Solder, Carl (2006). "Cisco Networkers"

Cisco Systems, Inc. (2007). "Infrastructure Protection on Cisco Catalyst 6500 and 4500 Series Switches."

Cisco Systems, Inc. (2009). "Configuring DHCP Snooping"

Cisco Systems, Inc. (2009). "Configuring Dynamic ARP Inspection."

Cisco Systems, Inc. (2009). "Design Zone for Security."

Hodgdon, Scott (2009). "CSSTG SE Residency Project Plan."

Cisco Catalyst 6509E Configuration

(Mitigation configured)

MAC Address Overflow Attack



```
enable password xxxxx
Т
no aaa new-model
ip subnet-zero!
!
        !
! Configuration for enabling DHCP Snooping
ip dhcp snooping vlan 7
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
!
!
! Configuration for enabling Dynamic ARP Inspection (DAI)
ip arp inspection vlan 7
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
! Because we are using a Static IP Address in Scenario 1, we must configure
! a source binding since we have enabled DHCP Snooping and Dynamic
! ARP Inspection (DAI). This will bind the MAC address on the NIC on the
! Attacker Machine to the static IP address connected to port GE1/2 on vlan 7
ip source binding 0023.6948.B89C vlan 7 10.1.0.60 interface Gi1/2
I.
ī
!
```

```
! The following command limits the number of accepted MAC addresses
! inbound on port GE1/2 (Attacker Machine) to 15.
mac-address-table limit interface gi1/2 maximum 15 action limit
!
!
vtp domain CISCO
vtp mode transparent
mls netflow interface
no mls flow ip
mls cef error action reset
Т
redundancy
keepalive-enable
mode sso
main-cpu
 auto-sync running-config
spanning-tree mode pvst
!
!
| * * * * * * *
                            ! The "errdisable recovery cause all" command will automatically add the following
configuration
! commands to the switch
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause gbic-invalid
errdisable recovery cause 12ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
```

```
errdisable recovery cause unicast-flood
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause link-monitor-failure
errdisable recovery cause oam-remote-failure
errdisable recovery cause loopback
errdisable recovery interval 30
fabric timer 15
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
T.
vlan 7,10,20
!
vlan 50
remote-span
!
vlan 255
!
!
I
L
! Victim 2 connected to GE1/1. Victim 2 is a MacBook Pro running OS X 10.5.7. The
! IP address of Victim 2 is 10.1.0.61/24. This static IP address has been excluded
from
! the DHCP Server's IP Pool of addresses.
interface GigabitEthernet1/1
switchport
switchport access vlan 7
switchport mode access
1
```

```
! GE1/2 Connected to "Attacker" Ubuntu 9.04 Virtual Machine running on the
! MacBook Pro inside VMware Fusion. The Ubuntu 9.04 Attacker Machine will
! have an IP address of 10.1.0.60/24. Note that this static IP address is excluded
! from the DHCP Server's IP Pool of addresses.
interface GigabitEthernet1/2
switchport
switchport access vlan 7
switchport mode access
!
interface GigabitEthernet1/3
 switchport
switchport access vlan 7
switchport mode access
shutdown
!
interface GigabitEthernet1/4
no ip address
shutdown
!
interface GigabitEthernet1/5
no ip address
shutdown
!
interface GigabitEthernet1/6
no ip address
shutdown
ı.
Т
interface GigabitEthernet1/7
no ip address
shutdown
!
interface GigabitEthernet1/8
no ip address
shutdown
```

```
!
interface GigabitEthernet1/9
no ip address
shutdown
!
interface GigabitEthernet1/10
no ip address
shutdown
ı.
interface GigabitEthernet1/11
no ip address
shutdown
!
interface GigabitEthernet1/12
no ip address
shutdown
!
! GE1/13 is connected to Victim 1, the Lenovo PC running Windows XP.
! It has an IP address of 10.1.0.51/24.
interface GigabitEthernet1/13
switchport
switchport access vlan 7
switchport mode access
!
interface GigabitEthernet1/14
switchport
switchport access vlan 7
switchport mode access
shutdown
!
interface GigabitEthernet1/15
switchport
shutdown
!
interface GigabitEthernet1/16
```

```
no ip address
shutdown
!
interface GigabitEthernet1/17
no ip address
shutdown
interface GigabitEthernet1/18
no ip address
shutdown
!
interface GigabitEthernet1/19
no ip address
shutdown
!
interface GigabitEthernet1/20
no ip address
shutdown
!
interface GigabitEthernet1/21
no ip address
shutdown
!
interface GigabitEthernet1/22
no ip address
shutdown
!
interface GigabitEthernet1/23
no ip address
shutdown
!
interface GigabitEthernet1/24
no ip address
shutdown
interface GigabitEthernet1/25
no ip address
shutdown
!
```

```
interface GigabitEthernet1/26
no ip address
shutdown
!
interface GigabitEthernet1/27
no ip address
shutdown
!
interface GigabitEthernet1/28
no ip address
shutdown
I.
interface GigabitEthernet1/29
no ip address
shutdown
!
interface GigabitEthernet1/30
no ip address
shutdown
interface GigabitEthernet1/31
no ip address
shutdown
!
interface GigabitEthernet1/32
no ip address
shutdown
!
interface GigabitEthernet1/33
no ip address
shutdown
!
interface GigabitEthernet1/34
no ip address
shutdown
!
interface GigabitEthernet1/35
no ip address
```

```
shutdown
!
interface GigabitEthernet1/36
no ip address
shutdown
!
interface GigabitEthernet1/37
no ip address
shutdown
!
interface GigabitEthernet1/38
no ip address
shutdown
!
interface GigabitEthernet1/39
no ip address
shutdown
!
I.
interface GigabitEthernet1/40
no ip address
shutdown
interface GigabitEthernet1/41
no ip address
shutdown
!
interface GigabitEthernet1/42
no ip address
shutdown
!
!
!
interface GigabitEthernet1/43
no ip address
shutdown
!
interface GigabitEthernet1/44
```

```
no ip address
shutdown
!
interface GigabitEthernet1/45
no ip address
shutdown
ı.
interface GigabitEthernet1/46
switchport
switchport access vlan 7
switchport mode access
I.
! GE1/47 connects to the Cisco 881 Router (port 0/5) that is acting as the external
! DHCP Server for scenario 2.
interface GigabitEthernet1/47
description *** Connects to 881 Router Acting as DHCP Server [10.1.0.200] port 0/5
* * *
switchport
switchport access vlan 7
switchport mode access
! Configuring GE1/47 as a trusted port for both DHCP Snooping and Dynamic ARP
! Inspection (DAI).
ip arp inspection trust
ip dhcp snooping trust
I.
interface GigabitEthernet1/48
switchport
switchport mode dynamic auto
I.
interface GigabitEthernet5/1
no ip address
shutdown
!
interface GigabitEthernet5/2
```

```
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
Т
! Victim 3 is Interface VLAN 7.
interface Vlan7
ip address 10.1.0.1 255.255.255.0
!
!
!
router eigrp 100
network 10.1.0.0 0.0.0.255
network 172.18.176.0 0.0.0.255
no auto-summary
!
ip classless
!
no ip http server
no ip http secure-server
!
control-plane
!
dial-peer cor custom
!
alias exec sdsb show ip dhcp snooping binding
!
line con 0
exec-timeout 0 0
line vty 0 4
session-timeout 800
password 12345
```

```
login
length 0
transport preferred none
transport input all
transport output none
line vty 5 15
login
transport input lat pad udptn telnet rlogin ssh
!
scheduler process-watchdog terminate
scheduler switch allocate 1000 1000
scheduler allocate 400 100
mac-address-table aging-time 480
!
end
```

Appendix

Introduction to Ubuntu Install Guide for L2 Attack Tools

This appendix is intended for those users that are not familiar with the Ubuntu Linux OS and want to be able to quickly download and use the Layer 2 attack and monitoring tools (Ettercap, Yersinia, packETH and Wireshark) that are utilized throughout these series of Layer 2 attack whitepapers. The Synaptic Package Manager in Ubuntu is the GUI application for installing software packages in the dpkg format with the file extensions of ".deb." This dpkg format was the first Linux packaging to integrate dependency information. The Debian Package Mgmt. system database tracks which software packages are installed, which version is installed, and other packages that it is dependent on. This allows you to automatically identify, download, and install all dependent applications that are part of your original application installation selection. The Synaptic Package Manager to point to those dpkg repositories that are supported by Ubuntu, you must add those repositories to /etc/apt/sources.list.

This appendix covers the complete installation of the Ettercap application, modification of its initial configuration file (parameter values that provide privilege level, rerouting capabilities, remote browser capabilities, etc to ettercap) and where and how to launch the application. The other L2 attack and monitoring tool installations (Yersinia, packETH and Wireshark) are not covered in their entirety as the process is similar. These applications do differ in where and how they are launched and the appendix will cover these unique differences in detail.

Listed below is a summary of the different attack scenario's and which L2 attack tools were used:

- STP MiTM (Vlan) Attack: Yersinia, Ettercap, Wireshark
- STP MiTM (ISL) Attack: Yersinia, Ettercap, packETH, Wireshark
- ARP MiTM Attack: Ettercap, Wireshark
- MAC Overflow Attack: Ettercap, Wireshark
- DHCP Consumption Atack: Yersinia, Wireshark

Ettercap

Ettercap Installation via Synaptic Package Manager

Select "System>Administration>Synaptic Package Manager" to load Synaptic; the GUI application to download, install and remove applications on Ubuntu Linux.

Figure 31.



You will be required to enter your password to perform Administrative Tasks such as installing software.

Figure 32.

U. T	The applica	tion 'Synapti	c Package Ma	namer' lets vo
r	nodify ess	ential parts o	f your system	tinger reis ye.
F	assword:			

Type "**ettercap**" in the Quick Search Field and the Synaptic Package Manager will locate the application for installation.

Figure 33.

C S Reload Mark All Upgrade	85	Apply Properties	ttercap	Ý
All	S	Package	Installed Version	Latest
Amateur Radio (universe)		ettercap		1:0.7.3
Base System		ettercap-common		1:0.7.3
Base System (restricted) Communication		ettercap-gtk		1:0.7.3
Communication (multivers	121	-	AND STREET	5
Communication (restricted	No	package is selected.		
Sections				
S <u>t</u> atus				
Origin				
Qustom Filters				

Select the "ettercap-gtk" application for the GUI version of Ettercap by left clicking your mouse on the application.

Figure 34.

5	ynaptic Package Manager	
<u>Eile Edit Package Settin</u>	gs Help	
C S Reload Mark All Upgrad	les Apply Properties	ouick search ettercap
All	S Package	Installed Version Latest
Amateur Radio (universe)	ettercap	1:0.7.
Base System	ettercap-common	1:0.7.
Base System (restricted)	ettercap-gtk	1:0.7.
Communication	4	
Communication (multiverse	(
Communication (restricted	Multipurpose sniffer/in switched LAN	nterceptor/logger for
Sections	Get Screenshot	-
Status	This package includes gtk e	nabled version of ettercap. It
Origin	also includes process support	
Custom Filters		
	Ettercap supports active and	passive dissection of many

Left click on "Mark for Installation."

Figure 35.

8 5)	naptic Package Manager	10	
Eile Edit Package Setting	is <u>H</u> elp		
<u>č</u> 😡	V 🔥 🖓	lick search	Ŷ
Reload Mark All Upgrad	es Apply Properties C	uercap	
All	S Package	Installed Version	Latest
Amateur Radio (universe)	ettercap		1:0.7.3
Base System	ettercap-common		1:0.7.3
Base System (restricted)	C attarras atta	1	1:0.7.3
Communication	U Unmark		
Communication (multivers	Mark for Installation	- N	>
Communication (restricted	Mark for Honrade	tor/logger for	
Communication (universe)	Mark for Removal		1947
Sections	Mark for Complete Remo	Vial	
Status	-	abled uppies of otherse	
Origin	also	abled version of ettercap	
Custom Filters	includes neurses support.		
Search Results	Ettercap supports active and protocols	passive dissection of ma	ny 🚽

Additional application dependencies have been identified. Mark this additional application for installation.

Figure 36.

The chosen action also The following changes proceed.	affects other packages. are required in order to
To be installed ettercap-commo	n

Ettercap has been marked along with its application dependency on "**ettercap-common**." Go ahead and hit "**Apply**" to install both applications.

Figure 37.

8	Syn	aptic Packa	ge Manager	r (
<u>File Edit Package Set</u>	tings	Help			
è 💽		140		Quick search	
Reload Mark All Upg	rades	Apply	Properties	ettercap	~
All	A	S Packag	e	Installed Version	Latest
Amateur Radio (universe)		etterca	р		1:0.7.3
Base System	(S etterca	p-common		1:0.7.3
Base System (restricted)	1	5 etterca	p-gtk		1:0.7.3
Communication					
Communication (multiver	s t	<)
Communication (restricted		Multipurp	ose sniffer	/interceptor/logger fo	or 👘
		switched	LAN		=
Sections	3	Get Screen	shot		_
Status		This see how	to de la composition	la marking and an and a barre	
Origin		also	je maiudes gu	k enabled version of etterc	abrit
engin	_	includes not	irses support.		
Custom Filters					
Search Results		Ettercap sup protocols	ports active a	and passive dissection of m	hany v

3 packages listed, 1216 installed, 0 broken. 2 to install/upgrade, 0 to remove; 1794 kB will be used

Hit "Apply" in the summary screen to confirm your installation selections.

Figure 38.



When your installation is complete, the "Changes applied" window will pop up. Close this window to proceed.

Figure 39.



Synaptic will indicate that the applications have been successfully installed by the filled green boxes next to the application.

Figure 40.

s Sy	naptic Package Manager	
<u>File Edit Package S</u> etting	s <u>H</u> elp	
Contraction Reload Mark All Upgrade	s Apply Properties Qui	ck search ercap ~
All	S Package	Installed Version Latest
Amateur Radio (universe)	ettercap	1:0.7.3
Base System	ettercap-common	1:0.7.3-1.2ubuntu4 1:0.7.3
Base System (restricted)	ettercap-gtk	1:0.7.3-1.2ubuntu4 1:0.7.1
Communication		R
Communication (multivers	c	1
Communication (restricted	Multipurpose sniffer/into switched LAN	erceptor/logger for
Sections	Get Screenshot	
S <u>t</u> atus	This package includes gtk ena	bled version of ettercap. It
Origin	also	
<u>C</u> ustom Filters	includes ncurses support.	
S <u>e</u> arch Results	Ettercap supports active and p	assive dissection of many

Modification of Ettercap initialization file "/etc/etter.conf"

We are going to use the terminal shell to modify the **"/etc/etter.conf**" file. Select **"Applications>Accessories>Terminal**" to open a terminal window.

Figure 41.



When the terminal window opens, type "**sudo gedit** */etc/etter.conf*" to open the file with the appropriate privileges to modify the file. You will be prompted for the root password to continue.

Figure 42.



The "ec_uid" and "ec_gid" values both need to be changed to "0" to provide the appropriate privilege level to Ettercap upon execution. The default values are "65534." Change these to "0" as depicted below.

Figure 43.

2	etter.conf (/etc) - gedit	
Eile Edit View Search Jos	ols Documents Help	
New Open - Save Print.	Undo Fedo Cut Copy Poste Find Replace	
etter.conf 😕		
[privs]		2
ec uid = 0 ec uid = 0	# nobody is the default # nobody is the default .	-
	h	
<pre>(alim) arp_storm delay = 10 arp_poison_warm_up = 1 arp_poison_icmp = 1 arp_poison_icmp = 1 arp_poison_reply = 1 arp_poison_request = 0 arp_poison_equest = 0 arp_poison_equest = 1000 port_steal_delay = 10 port_steal_send_delay = 1</pre>	<pre># milliseconds # seconds # seconds # boolean # boolean # boolean # boolean # seconds # milliseconds # milliseconds</pre>	
[connections] connection timeout = 300 connection idle = 5 connection buffer = 18080 connect_timeout = 5	# seconds # seconds # bytes # seconds	
	Plain Text - Tab Width: 8 - Ln 19, Col 1 IN	S

The "**port_steal_send_delay**" value needs to be changed to "1" microseconds. The default value is "2000" microseconds for the port steal send delay. We need to populate arp tables faster than Cisco's default ARP table timeout values can clear them.

Figure 44.

2	etten.conf (/etc) - gedit 👘 🔚 🗉	*
Eile Edit View Search To	ols Documents Help	
New Open ~ 🔛 🔒	Undo Redo Cut Copy Paste Find Replace	
🗏 etter.conf 🧧		
[privs]		6
ec uid = 0	≠ nobody is the default	
ec_gid = 0	# nobody is the default	E
Inital		
arn storm delay = 19	# milliseronds	
arn poison warn un = 1	# seconds	
arp poison delay = 10	# seconds	
arn noison icmn = 1	# boolean	
arp poison reply = 1	# boolean	
arp poison request = 0	# boolean	
arp poison equal mac = 1	# boolean	
dhcp lease time = 1800	# seconds	
port steal delay = 10	# milliseconds	
port steal send delay = 1	# microseconds	
in the second	A.	
[connections]	1. C.	
connection timeout = 300	# seconds	
connection idle = 5	# seconds	
connection buffer = 10000	# bytes	
connect timeout = 5	# seconds	~
	Plain Text v Tab Width: 8 v Ln 31 Col 1 INS	- Canada

Comment out "#" the original remote browser command line and add the remote_browser command line as entered below—mozilla is replaced with firefox. This fixes the MiTM remote browsing plugin within ettercap. This enables us to view the same web pages as a victim in real time.

Figure 45.



Uncomment the iptables commands by removing the "#" symbol. This will allow you to reroute traffic when performing a MiTM attack on behalf of the gateway and the victim.

Figure 46.

L2					ttencor	if (/etc) - ged	ili:				-	8
Eile	<u>E</u> dit	⊻iew	<u>S</u> earcl	h <u>T</u> oo	s Doci	iments	<u>H</u> elp						
New) Open	~ [] Sa	e ve	Print	Unde	Redo	Cut	Сору	Paste	E. Find	Replace	e	
🔄 ett	ter.conf	13											
<pre># # # f f f f port f port f redir port redir f f f f f f f f f f f f f f f f f f f</pre>	Vou us redir c -j RED redir c -j RED you us comma -j RED r comma	e ipcl ommand IRECT ommand IRECT e ipt nd on IRECT nd of	hains d_on %rpo d_off %rpo ables = "i to f = "	i = "ipc rt" = "ip rt" : ptable -port iptabl	hains - chains s -t na %rport" es -t n	A inpu -D inp t -A P at -D	t -i S ut -l REROUT PREROU	iface %iface ING -1 TING -	-p tcp - p tc : %ifac i %ifa	-s 0/ p -s 0 e -p t ce -p	0 -d 0/ /0 -d 0 cpdp tcpd	0 % N/O % Nort %	
port	-] RED	IRECT	to	-port	srport"					h	8		-
#										100			h
#	Mac Os	Х											
#		*****											
# qui #r	ick and redir c	dirty	y way d on :	: = "ipf	w add f	wd 127	.0.0.1	,%rpoi	rt top	from a	ny to a	inγ %	¥
					Plain T	ext ~	Tab Wi	dth: 8	- Ln 1	70. Col	1	INS	

When you have completed these modifications, hit the "save" tab at the top of the editor.

Figure 47.



Launching Ettercap

Ettercap can be launched from "**Applications>System Tools**" or you can right click on "**ettercap**" from "**System Tools**" and install a launcher to the desktop.

Figure 48.



Ettercap can now be launched from the Ubuntu Desktop.

Figure 49.

Applications	Places	System	0	
Wireshark (as n	oot)			
Terminal				
ettercap				

Double clicking on the Ettercap icon launches the following Ettercap application.

Figure 50.



Yersinia

Yersinia Installation via Synaptic Package Manager

Follow the same process as outlined in Figures 53 to 62 to install the Yersinia (Figure 73) application. The below figure depicts the currently installed application—as denoted by the green box next to the application.

Figure 51.

s	ynaptic Package Manager		
<u>File E</u> dit <u>P</u> ackage <u>S</u> ettin	gs <u>H</u> elp		
C IV Reload Mark All Upgrad	les Apply Properties	Quick search yersinia	Ŷ
All	S Package	Installed Version	Latest
Amateur Radio (universe) Base System Base System (restricted) Communication	yersinia	0.7.1-1	0.7.1-1
Communication (multiverse	K		>
Communication (universa)	No package is selected.		
Sections			
Status			
Origin			
<u>C</u> ustom Filters			
	1		

Launching Yersinia's Graphical Interface

Yersinia must be launched from a terminal window. Click on "**Applications>Accessories>Terminal**" to open a terminal window.

Figure 52.

Applications Place	ces S	ystem 🎯 🖂 🕢	ab
Accessories	>	Calculator	
🚯 Games	>	CD/DVD Creator	
🔏 Graphics	>	G Character Map	
linternet	>	🔊 Disk Usage Analyzer	
0ffice	>	🔛 Manage Print Jobs	
🛐 Sound & Video	>	net the second state of the second se	
System Tools	>	📷 Take Screenshot	
Add/Remove		Terminal	
() restriction		Text Editor	
		Z Tomboy Notes	
Interfaces config.odt			

Give the terminal window root privilege by typing the command "**sudo su**" at the command prompt. You will be required to provide a root password. There are several different options to launch yersinia from the CLI—"-G " for Graphical or "-I" for interactive. The "**yersinia** –**G**" option loads the Graphical version of Yersinia depicted in Figure 75.

Figure 53.



The default Yersinia screen when using the Graphical option for launching the application.

Figure 54.

	Yersinia 0.7.1
Bie Protocols Actions Optio	ins Help
Launch attack	Load default. List attacks Clear stats Capture Edit mode Exit
Protocols Packets	DP DHCP 802.10 802.1X DTP HSRP ISL STP VTP Versinia log
COP 0 DHCP 0 602.10 0 802.11X 0 DTP 0 HSRP 0 ISL 0 STP 0 TYP 0 TYP 0	TL DevID Interface Count Lost seen
Field Value Description	Isco Discovery Protocol Aurce MAC 06:43:88:68:41:50 Destination MAC 01:68:8C:CC:CC Extra ersion 01 TTL 54 Checksum 9898
12:33:31	

Launching Yersinia's Interactive Interface

To launch the Interactive interface of Yersinia, you must be using a full size terminal window. Make sure you maximize your terminal session before launching the application with the "-I" option.

Figure 55.

File Edit View Terminal Help. Klauerma@Ubuntu-Desktop:~\$	Window
klauerma@Ubuntu-Desktop:~\$	
€	

Once the window is maximized launch Yersinia with the "-I" option from the CLI.

Figure 56.

Applications Places System 🔯 📄 🚱		#) Mon Aug 31, 12:52 PM	Kevin Lauerman
	roota Ubanto: Desktopi /home/klauerma		
le Edit View Terminal Help			
uurmağUbuntu-Desktop:-\$ sudo su st@Ubuntu-Desktop:/hame/klauerma≢ yersinia -1 b			

If your window was not maximized, you will receive the error message depicted below.

Figure 57.



The initial dialog screen informs you that eth0 has been selected as the default interface. You have an option to load an additional Ethernet interface if desired or to change the default interface. Hit any key to proceed.

Figure 58.

[- Notification window Warning: interface eth0 sel - Press any key to continue -	ected as the default one		
	K			
1	Total Packets: 0 ————	STP Packets: 0	- MAC Spoofing [X] -	
	Source NAC 04:08:20:12:A9:75 Id 0000 Ver 00 Type 00 Flags Sridgeld 8423.18231602FF08 P	Destination NAC 01:80:C2:00:0 00 Rootid AC58.E7CD90117CAA ort 8002 Age 0000 Max 0014 Hel	00:00 Pathcost 00000000 Llo 0002 Fwd 000F	

Type a lower case "**h**" to pull up the help screen of available commands. This is just another interface for using Yersinia. Our examples of L2 attacks all use the Graphical version of Yersinia. This should be enough to get you going if you choose to use the Interactive interface to Yersinia.

Figure 59.



packETH

packETH Installation via Synaptic Package Manager

Follow the same process as outlined in Figures 53 to 62 to install the packETH (Figure 82) application. The below figure depicts the currently installed application—as denoted by the green box next to the application.

Figure 60.

5 S	naptic Package Manager/		
Eile Edit Package Setting	ıs <u>H</u> elp		
🍪 😡 Reload Mark All Upgrad	es Apply Properties	Quick search	~
All	S Package	Installed Version	Latest
Amateur Radio (universe) Base System Base System (restricted) Communication Communication (multiverse)	packeth	1.6-2	1.6-2
Communication (restricted	No package is selected.		
Sections			
S <u>t</u> atus			
Origin			
Custom Filters			
Search Results	T .		

Launching packETH

packETH must be launched from a terminal window. Click on "Applications>Accessories>Terminal " to open a terminal window.

Figure 61.

Accessories	>	Calculator	
🚯 Games	>	Ø CD/DVD Creator	
🔏 Graphics	>	🗴 Character Map	
🧿 Internet	>	🔊 Disk Usage Analyzer	
Office	>	🚔 Manage Print Jobs	
🗓 Sound & Video	>	🐲 Passwords and Encryption Keys	
🛞 System Tools	>	💼 Take Screenshot	
Add Bemove		Terminal	
() Hadricine ten	1112	Text Editor	
		Tomboy Notes	

Give the terminal window root privilege by typing the command "**sudo su**" at the command prompt. You will be required to provide a root password. Once you have root privilege, type "**packeth**" at the command prompt and hit enter.

Figure 62.



This is a partial view of the default window that appears for packETH upon launching. You will notice that this packet generator supports ver II, 802.3 and 802.1q frames.

Figure 63.

1	PackETH - e	thernet packet generator		*
File Help				
Builder Gen-t	Gen-s Pcap	Interface		
Link layer				
🖲 ver II	MAC Header Destination Select	802.10 VLAN fields	802.3 LLC field values Type @ LLC @ LLC-SNAP	
0 802.3	Source Select	Tag ID 0x 8100	DSAP 0x AA SSAP 0x AA Ctrl 0x 03 OUT 0x	
🗌 802.1q	Ethertype 0x 0800 IPv4 0	CR VLAN ID OX 001	PID 0x	
	Next layer> 🖲 IPv4	O Arp packet O User defined paylo	bad	
IPv4 data				-

Wireshark

Wireshark Installation via Synaptic Package Manager

Follow the same process as outlined in Figures 53 to 62 to install the Wireshark (Figure 86) application. The below figure depicts the currently installed application—as denoted by the green box next to the application. You will note that the Wireshark application is dependent on "**wireshark-common**." The Synaptic Package Manager will identify the dependency and prompt you to also install "**wireshark-common**."

Figure 64.

ile Edit Package Setting	gs <u>H</u> elp Qui	ick search	
Reload Mark All Opgrad	es appry i properties i	A	
All	S Package	Installed Version	Late
Amateur Radio (universe)	wireshark	1.0.7-1ubuntu1	1.0.7
Base System	wireshark-common	1.0.7-1ubuntu1	1.0.7
Base System (restricted)	tshark		1.0.7
Communication	wireshark-dev		1.0.7
Communication (multiverse	4 III	4	>
Communication (restricted	No package is selected.	0.	
< iii >			
Sections			
S <u>t</u> atus]		
Origin]		
	1		
Custom Filters			

Launching Wireshark

Wireshark can be launched from "**Applications>Internet>Wireshark (as root)**" by a single click or you can add the launcher to the desktop by right clicking on wireshark and then select "**Add this launcher to desktop**." The Wireshark icon can be double clicked from the Desktop to launch the application. Launched application is depicted in Figure 88.

Figure 65.



Figure 66.





Americas Haadquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquartera Cisco Systems (USA) Pic. Ltd. Singapore Europe Headquarters Cisco Systems Internetional BV Amaterciam, 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.

Oleop and the Oleop Logo are trademarks of Oleop Systems; Inc. and/or its affiliates in the U.S. and other countries. A listing of Oleop Indemarks can be found at reversion of the word partner does not imply a permetable trademarks between Oleop and any other company. [1009] (1009)

Printed in USA