## ARP Poisoning

## By: Christian Pervan

- Open three virtual machines : In this tutorial, you shall require a Kali 2.0 VM (we'll call this VM1), and two more VM's running operating systems Windows 7/8/8.1/10 (VM2 and VM3)
- On all 3 virtual machines, go to settings and make sure that the network adapter is set to NAT. This is important, you cannot set it to bridge or host only, it must be NAT. This is for all 3 machines.
- On VM1, open terminal and run "ifconfig". On VM2 and VM3, open up cmd and run "ipconfig". Take note of your IP address and MAC address on each of the respective machines.
- On VM3, go on the Internet and download a windows application XAMP. Download version "7.0.4 / PHP 7.0.4" under XAMPP for Windows on this page: <u>https://www.apachefriends.org/download.html</u>
- 5. Install XAMP using the downloaded installer file. Don not change any settings or check/uncheck any boxes. Just keep pressing "next" until you finish.
- 6. Once done installation, run XAMPP Control Panel on VM3. Once the main window pops up, start the Apache server by pressing he Start button on the Apache module row.
- To test the server, go on the internet on VM2 and type in <u>http://<insert VM3 IP here></u>. It should display a generic welcome page that looks like the following:



If successful, now go to VM1 (reminder – the one running Kali Linux 2.0. Arnold's should have the credentials root/toor). Go to applications and select "Applications > 09 – Sniffing & Spoofing > ettercap-graphical"



9. Go to Sniff > Unified Sniffing OR Pres Shift+U

File	Sniff Options ?		ettercap 0.8	8.0
	Unified sniffing	Shift+U	$\langle \Box \rangle$	
	Bridged sniffing	Shift+B		
	Set pcap filter	Р	~	
			T	
-		- tead	100	
			. \ .	
	//			
			ιl	、に

10. Select interface eth0

Network interface :		ettercap Input				
	_	~	eth0	Network interface :	?	
OK Cancel	_	Cancel	ОК			

11. Click Hosts > Scan for hosts



12. Click Hosts > Hosts List

	ettercap 0.8.0				
Start Targets	Hosts View Mitm	Filters Log	iging Plugins ?		
	Hosts list	н			
	Scan for hosts	Ctrl+S			
	Load from file	Ctrl+O			
F	Save to file	Ctrl+S 🚬	-		
1	A RUE				
		• • •			
		· 🕂 )			

13. From the new tab that appeared, you will see a list of IP's. Add the IP of VM3 to target #1 and add the IP of VM2 to target #2.

ettercap 0.8.0							
Start Targets Hosts Vi	iew Mitm Filters Logging	Plugins ?					
Host List 🗙							
IP Address MAC Ad	dress Description						
192.168.56.1 08:00:2	2:00:04:93						
192.168.56.100 08:00:2	7:F3:C6:29						
192.168.56.102 08:00:2	7:79:2092	<b>`</b>					
Delete Host	Add	to Target 1	Add to Target 2				
2182 known services							
Randomizing 255 hosts for s	Randomizing 255 hosts for scanning						
Scanning the whole netmask for 255 hosts							
Host 192 168 56 1 added to TARGET1							
105L 192.100.30.1 added to	0 TARGETI						
Host 192.168.56.102 added	d to TARGET2		=				

14. Go to Mitm > Arp Poisoning. In the pop up window that appears, only check "sniff remote connections" and press OK.

	ettercap 0.8	.0
Start Targets Hosts View	Mitm Filters Logging Pl	ugins
Host List 🕷	Arp poisoning	
	Icmp redirect	
IP Address MAC Addres	Port stealing	•
192.168.56.1 08:00:27:00	Dhep spoofing	
192.168.56.100 08:00:27:F5		
192.168.56.102 08:00:27:79	Stop mitm attack(s)	

15. Click on Start > Start Sniffing

ettercap 0.8.0						0.8.0	
Start	Targets	Hosts	View	Mitm	Filters	Logging	Plugins
Star	rt sniffing	Ctrl	+W ┥	<			
Stop sniffing		Ctr	l+E		Description		
Exit		Ctr	l+X or	0.04.93	Descrip		
192.168.56.100 08:00:27:				5:C6:29			
192.1	.68.56.10	2 08:00	0:27:79	9:2C:92			

- 16. Now go to "Applications > 09 Sniffing & Spoofing > wireshark"
- 17. Select eth0 and start scan
- 18. Now type in "arp" in the filters to only retrieve arp messages. Take note of the MAC addresses compared to the IP's. Also take note of the frequency of said messages
- 19. Now go to VM2 and repeat Step 7
- 20. Go back to VM1 and now type in a filter "ip.src==<VM2 IP>&&http" to get all http requests to server. You should notice there being 2 HTTP requests sent from VM2 to

VM3. However, take note of the MAC addresses. One of the requests should go from VM2 to VM1 and the next should go to from VM1 to VM3. If this is the case, you know we see a successful ARP poisoning.

- 21. Repeat step 20, just flip make VM3 the source IP and analyze all HTTP responses outgoing from the server. Similar idea, there should be two one going from VM3 to VM1 and another going from VM1 to VM2, but both in the name of VM3 to VM2 in the sniffed packets frame.
- 22. Congrats, you now know how to successfully ARP poison!