**Batch: B1 Roll No.: 16010121045**

**Experiment No. 6**

|  |
| --- |
| **Title:**  MITM and Session Hijacking using Ettercap, Ferret-sidejack, Hamster-sidejack/ Wireshark |

**Objective:**

MITM and Session Hijacking using Ettercap, Ferret-sidejack, Hamster-sidejack/ Wireshark

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO3** | Comprehend post exploitation phase of penetration testing. |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Books/ Journals/ Websites referred:**

1. [*https://www.hackingtruth.in/2020/03/session-hijacking-using-ettercap.html*](https://www.hackingtruth.in/2020/03/session-hijacking-using-ettercap.html)

**Introduction:**

**Man In the Middle (MITM) Attack:**

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers.

**Session Hijacking:**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connection. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server. The session token could be compromised in different ways; the most common are:

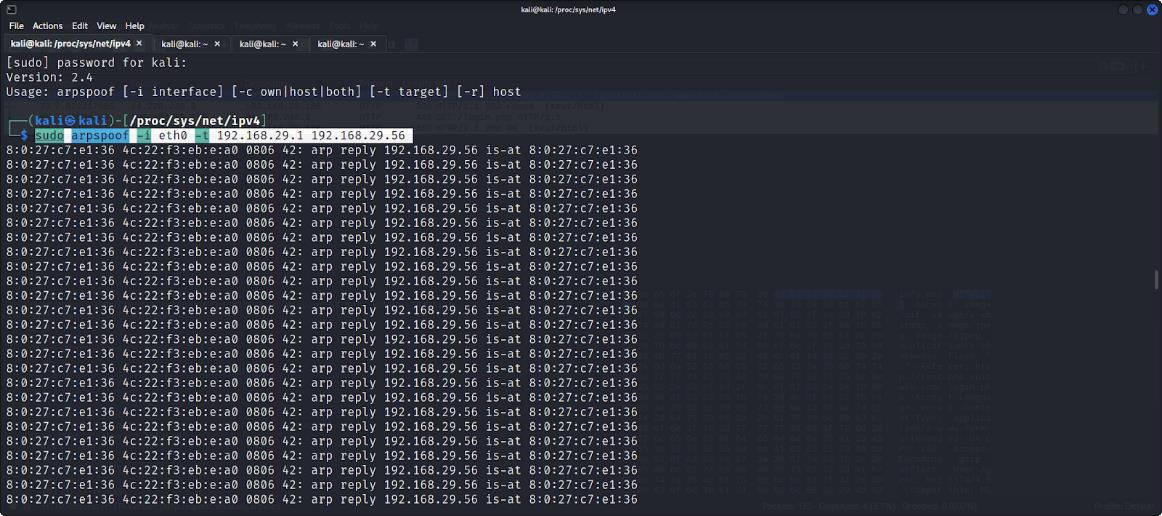
* Predictable session token
* Session Sniffing
* Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);
* Man-in-the-middle attack
* Man-in-the-browser attack

**Implementation details:**

Man In the Middle (MITM) Attack:

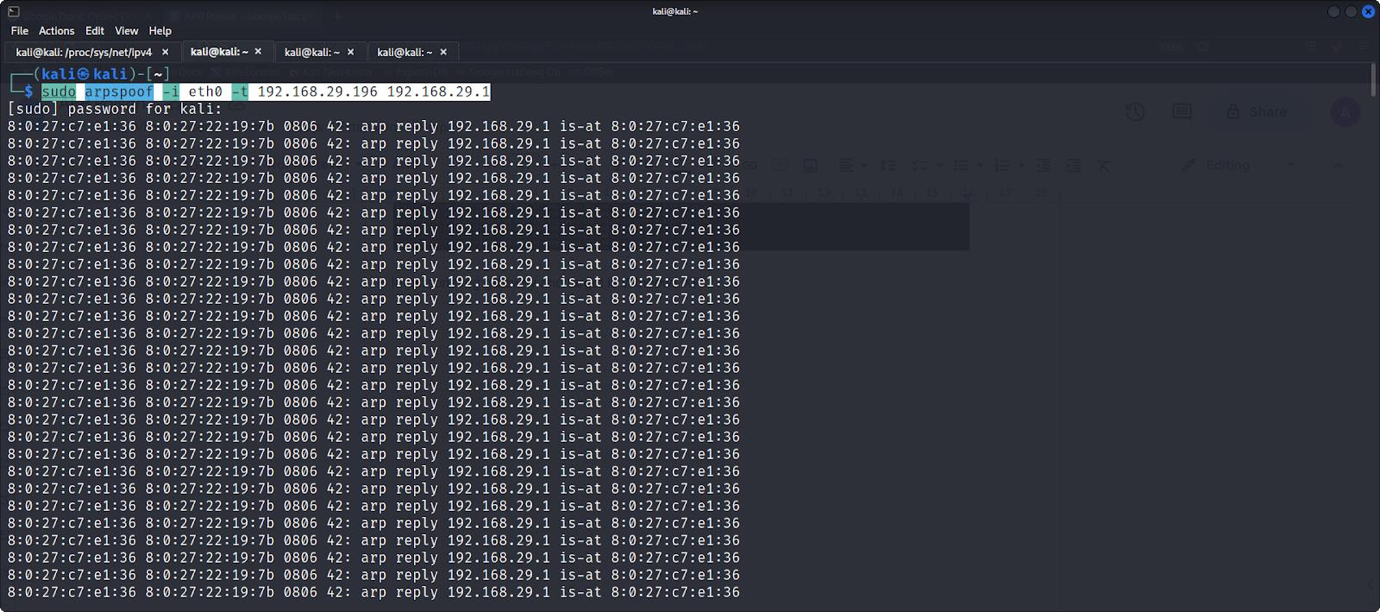
Here, the Target is gateway and we are Impersonating as Windows XP

*arpspoof -i eth0 -t 192.168.29.1 192.168.29.56*



In second tab, we impersonate as default gateway and our target is Windows XP

arpspoof -i eth0 -t 192.168.29.56 192.168.29.1

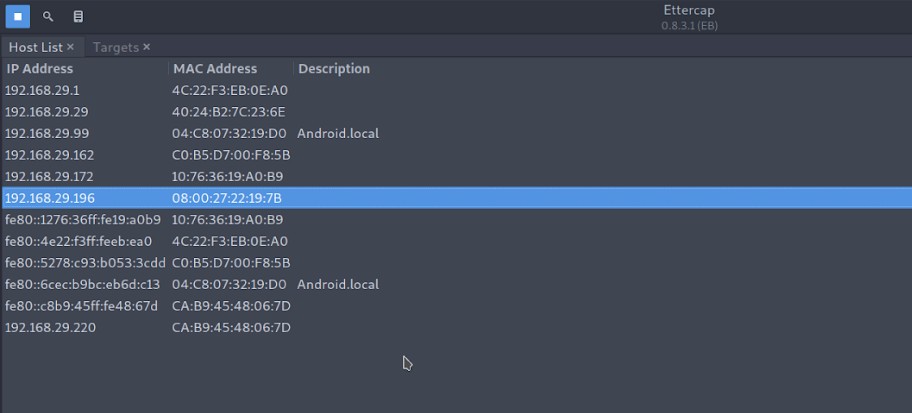


From Windows XP, we login to a vulnerable site and enter our credentials.

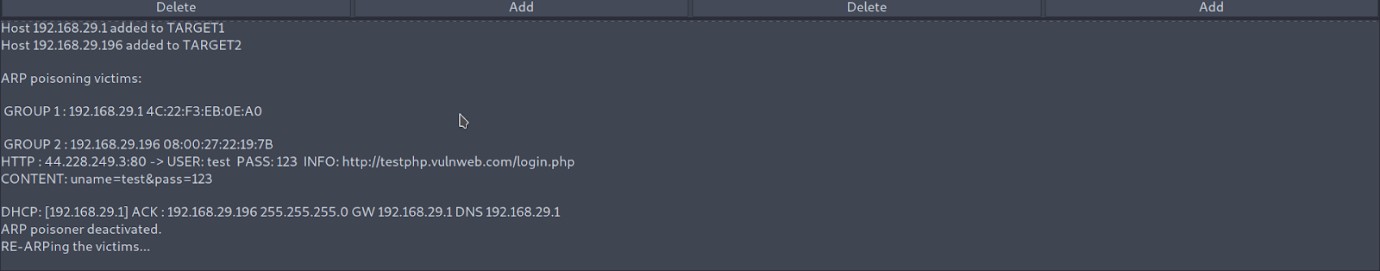
Capturing this traffic with Wireshark, we get the username and password in plaintext



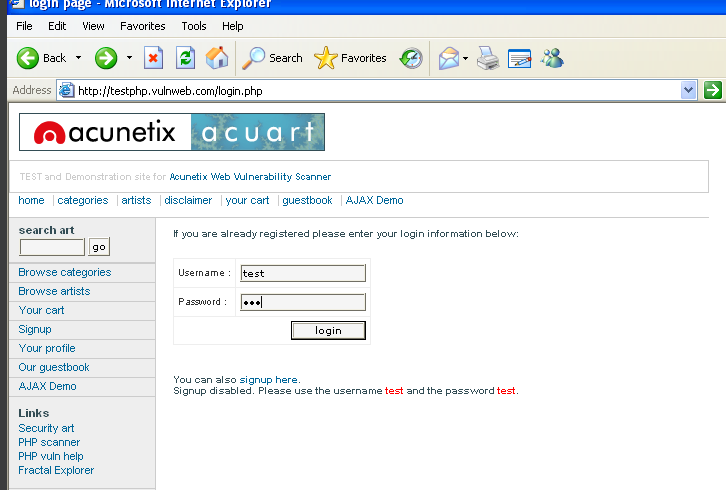
**Session Hijacking:**



Checking our Ettercap console



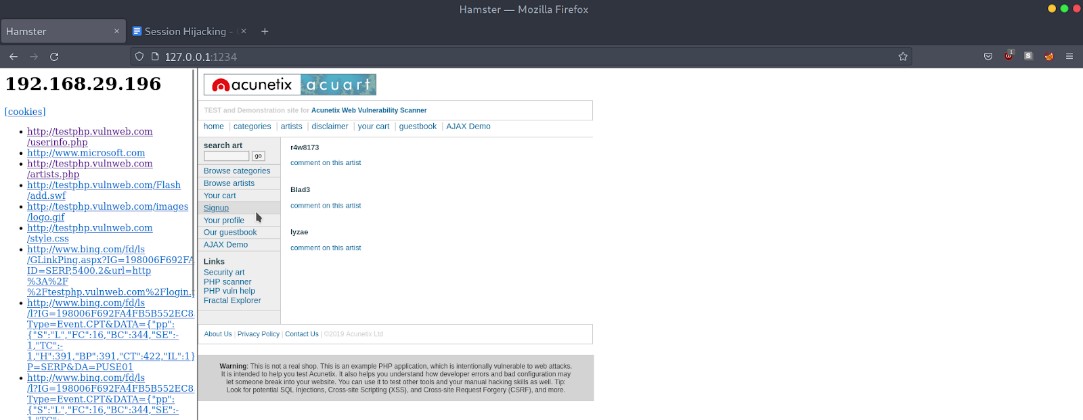
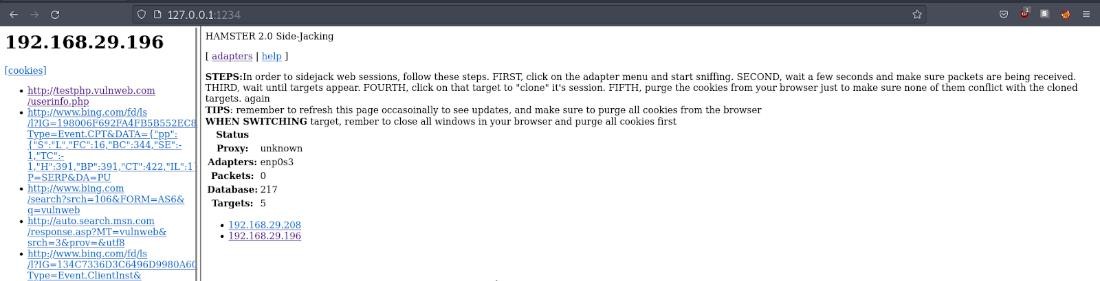
In our Windows XP machine, we open a http login form and enter credentials to see if ARP Poisoning is configured correctly



Now we visit the proxy given by hamster-sidejack tool (<http://localhost:1234>)



Now click on the IP address of Windows Machine at the bottom of page and you should see the cookies on left pane. Click the cookies to see the site



Now, we can see all the sites visited by the Windows Machine. Thus, we successfully performed session hijacking.

**Conclusion:** Through this experiment, I gained knowledge about session hijacking and man in the middle attack.