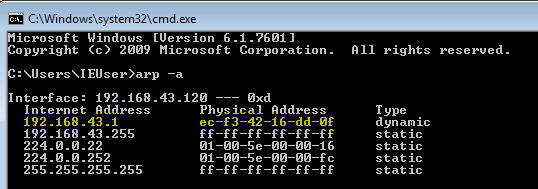
TABLE OF CONTENT

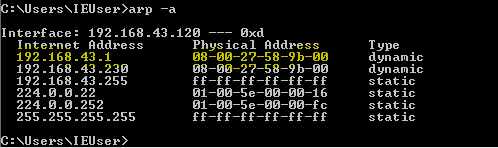
|  |  |  |
| --- | --- | --- |
| NO | INDEX | PAGES |
| 1. | ARP Spoofing | 3 |
| 2. | Install MITMF framework, Ferret and Hamster | 4 |
| 3. | Session Hijacking | 5-6 |
| 4. | Example of HTTPS session and cookies | 7-8 |
| 5. | References | 9 |

1. Before the mac address spoofed.



* Figure 1 show: Go to CMD and type arp –a.

1. After the mac address spoofed



* Figure 2 show: the mac address will be spoofed.

1. This is command for arp spoof



* Figure 3 show: arp spoof the gateway and -t <target ip>

1. This is command to reverse connection



* Figure 4 show: Tell the access point that I am the target client.

1. This is command for allow packet without packet lost



* Figure 5 show: Enable IP forward to allow packet to flow through our device without dropped.

1. Step to install MITMF FRAMEWORK

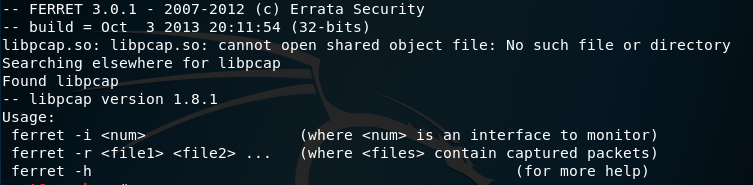




* Figure 6 show: After installation MITMF complete.

1. Step to install Ferret

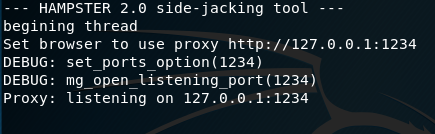




* Figure 7 show: After installation Ferret.

1. Step to install Hamster





* Figure 8 show: After installation and running the hamster look like above

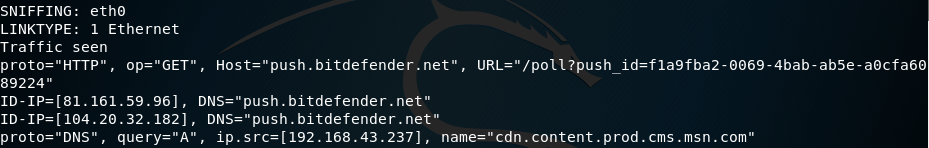
1. Open the MITMF



* Figure 9 show: Attacker doing men-in-the-middle the arp poisoning.

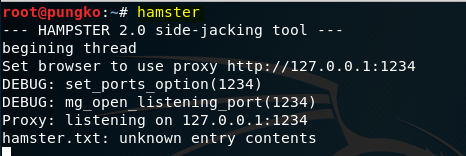
1. Open the Ferret





* Figure 10 show: ferret capture the cookies using interface eth0.

1. Open the Hamster

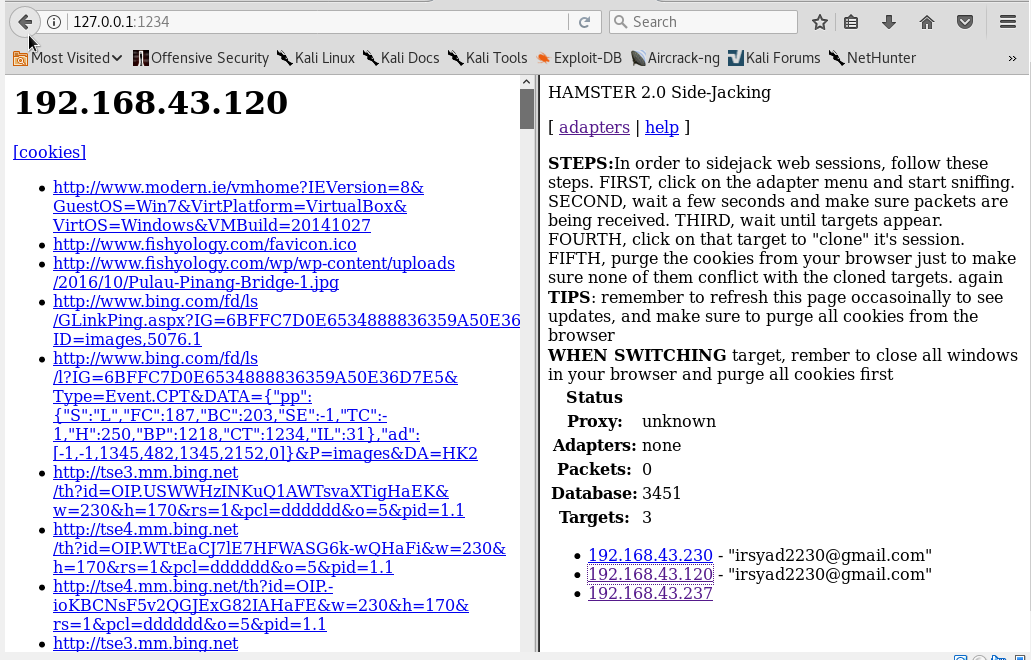


* Figure 11 show: hamster gui allows see the cookies and inject to the browser.

EXAMPLES OF HTTP COOKIES AND SESSION

Listen port

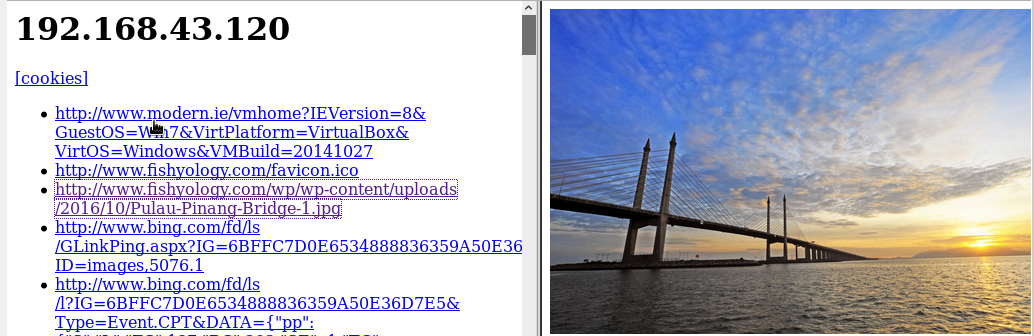
1. Open the Hamster type in url 127.0.0.1:1234



Victim ip address

* Figure 12 show: the cookies in the left side will capture and the Attacker will know the victim open search in google and etc.

1. This is example of cookies the Attacker get from the victim.



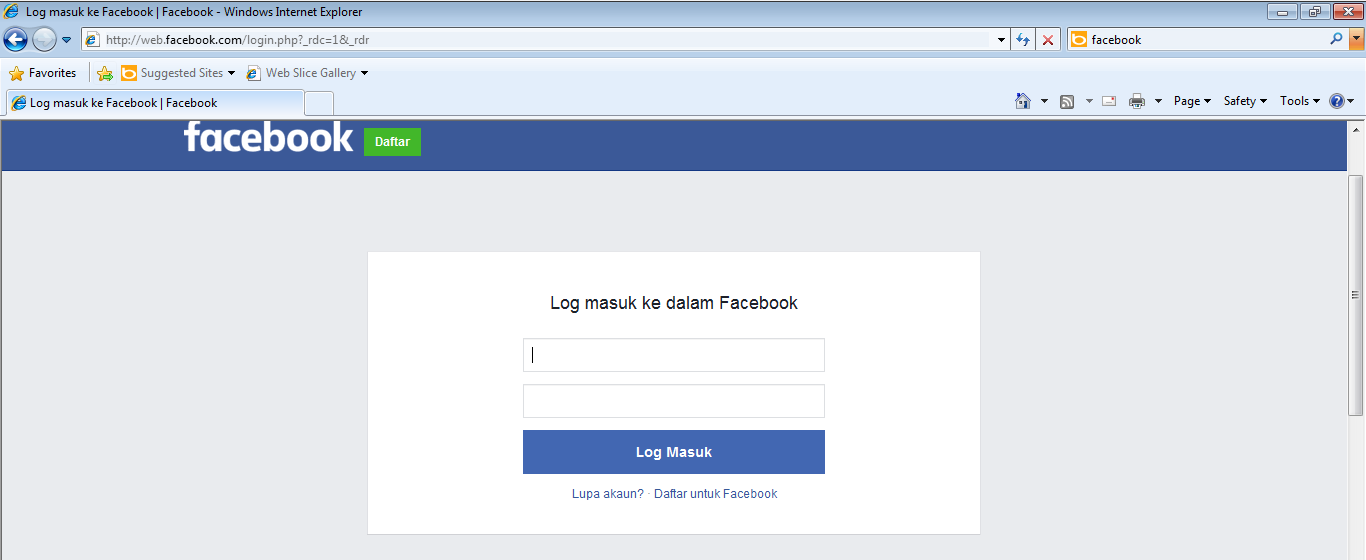
* Figure 13 show: the victim search in google image.

EXAMPLE OF HTTPS DOWNGREAD TO HTTP

1. Example of victim machine can show like this interface Facebook.com



HTTPS BROWSER TO HTTP



* Figure 14 show: MITMF able to downgread https to http.

1. Examples of Attacker using MITMF capture the username and password victim when victim try login to the Facebook.

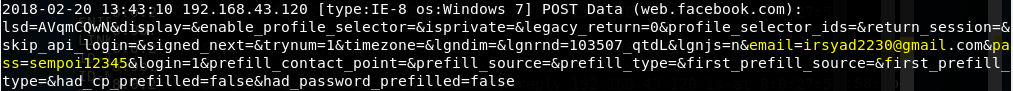


Figure 15 show: The username and password victim will be capture by attacker using MITMF.

1. Example victim search the [www.gmailsign.com](http://www.gmailsign.com)



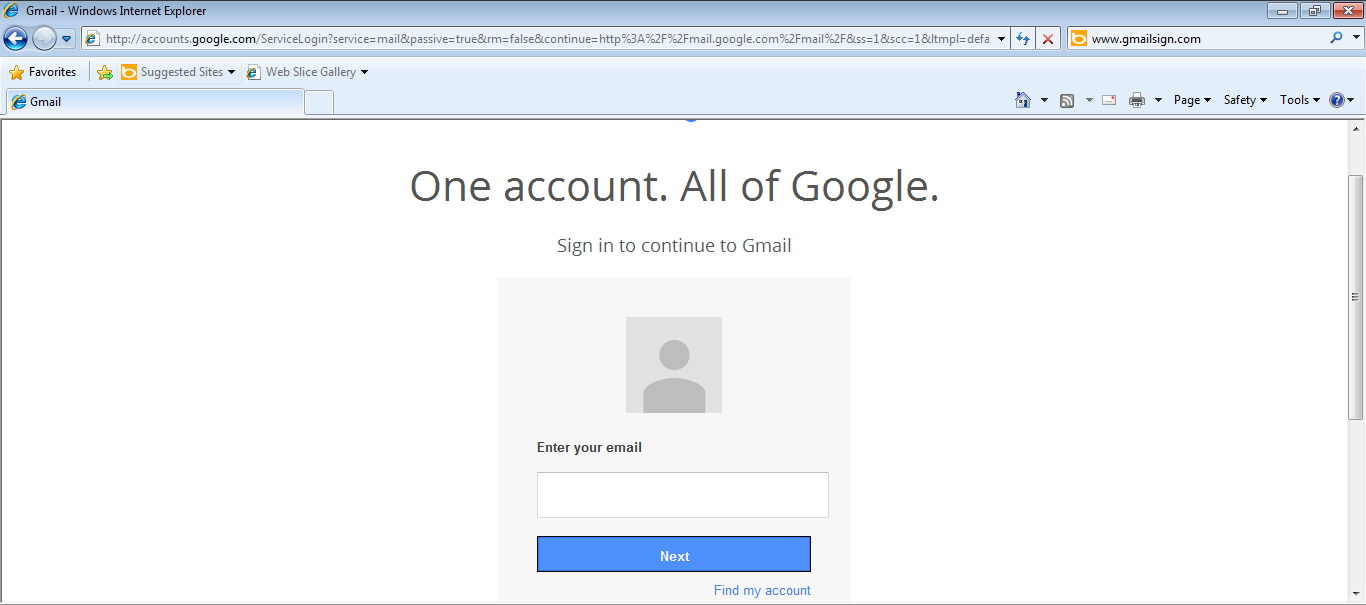


Figure 16 show: The victim cannot alert the url downgread https to http.

1. Example the Attacker capture the username and password when victim try log in to their account.

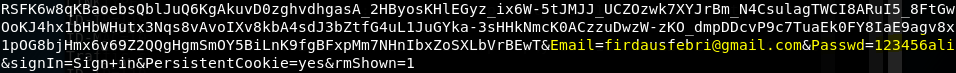


Figure 17 show: Attacker get the username and password by victim when victim try to log in to their account.

REFERENCE

1. https://github.com/
2. https://www.kali.org/