Session Hijacking

Module 11

Hijacking Sessions

Session Hijacking refers to the exploitation of a valid computer session, wherein an attacker takes over a session between two computers.

Lab Scenario

Source: **http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700**

According to Krebs on Security news and investigation, zero-day vulnerability in Yahoo.com that allows the attackers to hijack Yahoo! email accounts and redirect users to malicious Web sites offers a fascinating glimpse into the underground market for large-scale exploits.

The exploit, being sold for $700 by an Egyptian hacker on an exclusive cybercrime forum, targets a "cross-site scripting" (XSS) weakness in Yahoo.com that enables the attackers to steal cookies from Yahoo! Webmail users. Such a flaw would let attackers send or read email from victims' accounts. In a typical XSS attack, an attacker sends a malicious link to an unsuspecting user; if the user clicks the link, the script is executed that allows the attacker to access cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of HTML pages.

KrebsOnSecurity.com alerted Yahoo! to the vulnerability, and the company says it is responding to the issue. Ramses Martinez, director of security at Yahoo!, said the challenge now is working out the exact **yahoo.com** URL that triggers the exploit, which is difficult to discern from watching the video.

These types of vulnerabilities are a good reminder to be especially cautious about clicking links in emails from strangers or in unexpecting messages.

As a system administrator, you should implement security measures at the application and network levels to protect your network from session hijacking. Network-level hijacks are prevented by packet encryption, which can be implemented with protocols such as IPSEC, SSL, and SSH. IPSEC allows encryption of packets on a shared key between the two systems in communication.

Application-level security is obtained by using strong session IDs. SSL and SSH also provide strong encryption using SSL certificates to prevent session hijacking.

Lab Objectives

The objective of this lab is to help students learn session hijacking and take over a user account.

In this lab, you will:

- Intercept the Traffic between server and client
- Attain a user session by intercepting the traffic

Lab Environment

To carry out this, you need:

- A computer running Windows Server 2016 machine
- Kali Linux virtual machine
- Windows 10 virtual machine
- Web browser with Internet access
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 20 Minutes

Overview of Session Hijacking

Session hijacking refers to the exploitation of a valid computer session where an attacker takes over a session between two computers. The attacker steals a valid session ID, which is used to get into the system and sniff the data.

In TCP session hijacking, an attacker takes over a TCP session between two machines. Since most authentications occur only at the start of a TCP session, this allows the attacker to gain access to a machine.

Lab Tasks

Pick a website that you feel is worthy of your attention.

Recommended labs to assist you in session hijacking:

- Session Hijacking using the **Zed Attack Proxy** (ZAP)
- Perform sslstrip and Intercept HTTP Traffic through **BetterCAP**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Session Hijacking using the Zed Attack Proxy (ZAP)

The Zed Attack Proxy (ZAP) is an easy-to-use integrated penetration-testing tool for finding vulnerabilities in web applications.

It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

Lab Scenario

ZAP is an Intercepting Proxy. It allows you to see all the requests you make to a web app and all the responses you receive from it. Amongst other things, this allows you to see AJAX calls that may not otherwise be obvious. You can also set break points, which allow you to change the requests and responses on the fly.

Lab Objectives

The objective of this lab is to learn how to:

- Intercept the Traffic between server and client

Lab Environment

In this lab, you need:

- A computer running Windows Server 2016 as an Attacker machine
- Windows 10 running on virtual machine as a Target machine
- Owasp-ZAP located at **Z:\CEH-Tools\CEHv10 Module 11 Session Hijacking\Session Hijacking Tools\OWASP ZAP**
- You can also download the latest version of Owasp-ZAP from the link **https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Main**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A web browser with Internet access

- Administrative privileges to run this tool

Lab Duration

Time: 15 Minutes

Overview of Lab

This lab will demonstrate how to intercept the traffic of victims' machines by using a proxy, and how to view all the requests and responses that attackers receive from them.

Lab Tasks

1. Before starting this lab, we need to configure the **proxy** settings in the victim's machine. In this lab, **Windows 10** machine will be the victim machine.

2. Launch **Windows 10** virtual machine, **login**, and launch any browser. In this lab, we are using **Chrome** browser.

3. Once you launched **Chrome** browser, go to **Customize and control Google Chrome** button, and click **Settings** from the context menu.

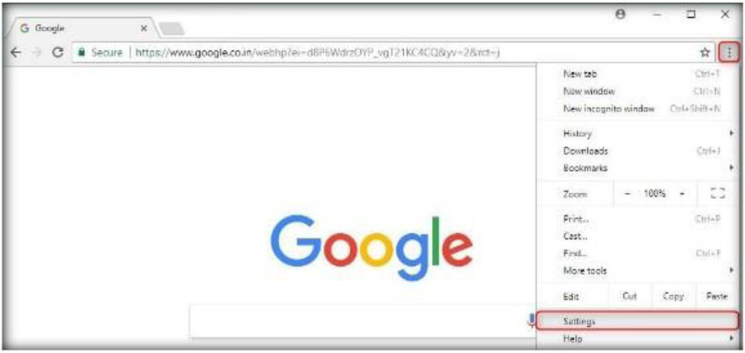
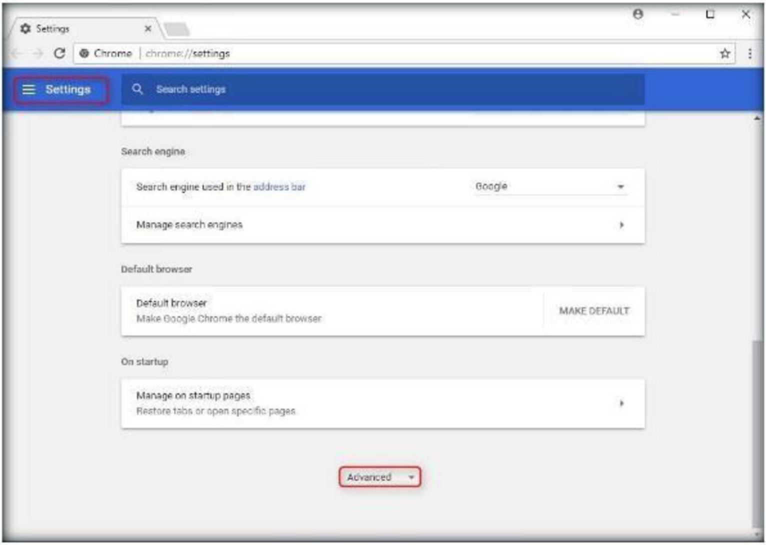


FIGURE 1.1: Google Chrome Settings

4. The **chrome://settings** window opens; scroll down to click **Advanced** in the browser.



Search engine

Search engine used in the address bar — Google

Manage search engines

Default browser

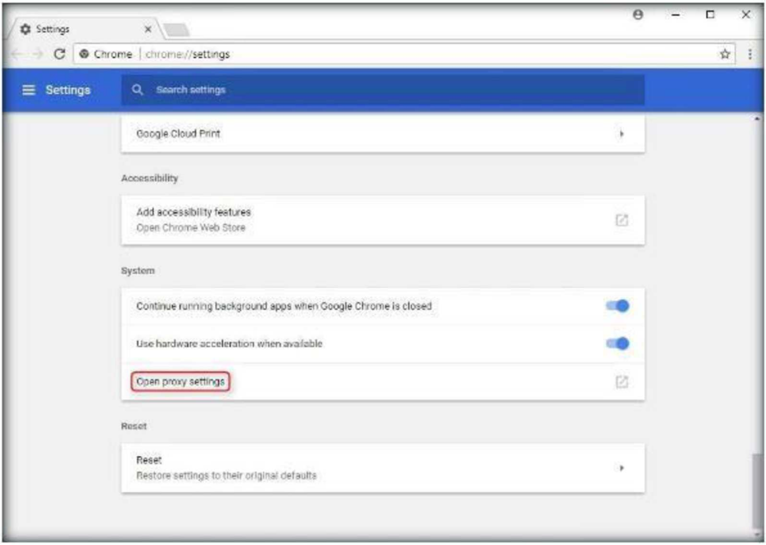
Default browser
Make Google Chrome the default browser — MAKE DEFAULT

On startup

Manage on startup pages
Restore tabs or open specific pages

FIGURE 1.2: Google Chrome Show advanced settings

5. In the **System** section, click **Open proxy settings** to configure a proxy.



Google Cloud Print

Accessibility

Add accessiblity features
Open Chrome Web Store

System

Continue running background apps when Google Chrome is closed — ●

Use hardware acceleration when available — ●

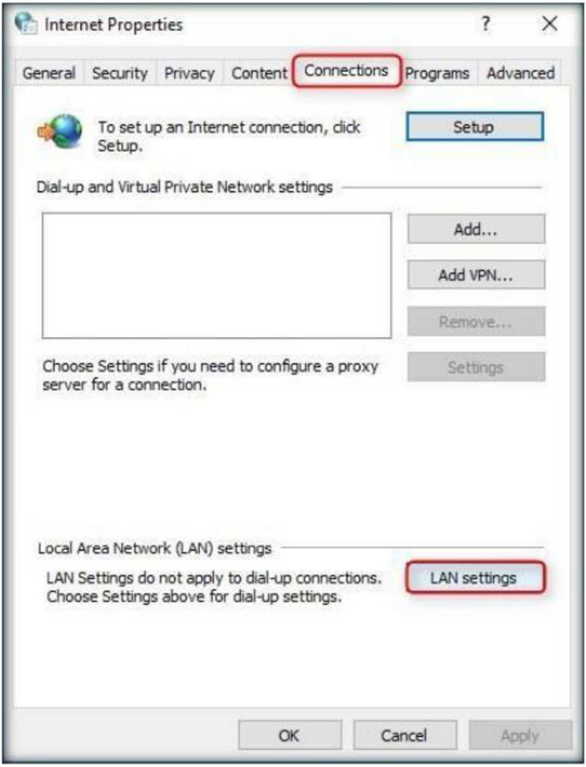
Open proxy settings

Reset

Reset
Restore settings to their original defaults

FIGURE 1.3: Google Chrome Change proxy settings

6. The **Internet Properties** pop-up window appears; click the **Connections** tab, and click **LAN settings** (under **Local Area Network (LAN) settings**).



Internet Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

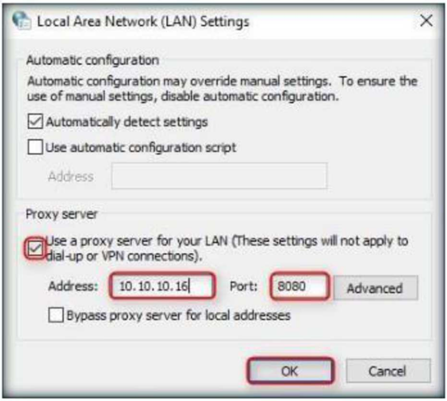
FIGURE 1.4: LAN Settings in Internet Properties

7. The **Local Area Network (LAN) Settings** pop-up appears; check **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).**

8. In the **Address** field, type the attacker machine's IP address, **8080** in the **Port** field, and then click **OK**.

9. In this lab, the attacker machine would be **Windows Server 2016**; its IP address is **10.10.10.16.**

   Note: The IP address shown in the lab will vary in your lab environment.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

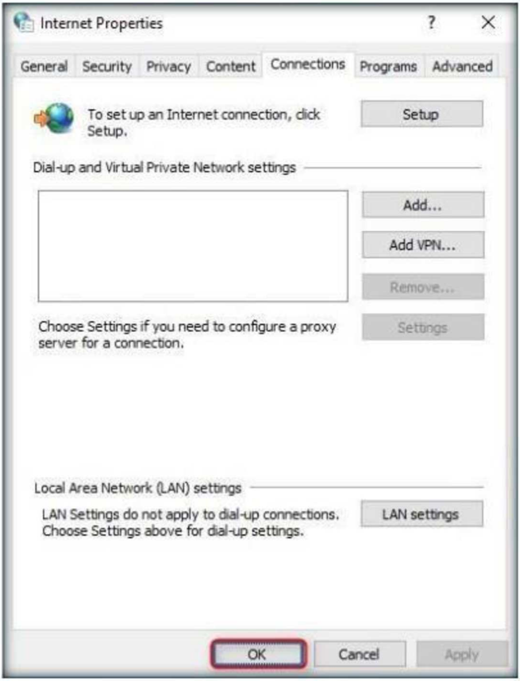
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 10.10.10.16 Port: 8080

□ Bypass proxy server for local addresses

FIGURE 1.5: Local Area Network (LAN) Settings

10. Once you have entered the required details, the **Internet Properties** pop-up window will appear; click **Apply**, and click **OK**.



Internet Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

FIGURE 1.6: LAN Settings in Internet Properties

11. Now you have configured victim machine proxy settings. Close the browser.

12. Switch to **Windows Server 2016** attacker machine and install OWASP-ZAP (Zed Attack Proxy).

13. Prior to installation, ZAP makes sure that **Java Run Time** is installed in your attacker machine (if not, you can navigate to **Z:\CEH-Tools\CEHv10 Module 11 Session Hijacking\Session Hijacking Tools\OWASP ZAP** and double-click **jre-8u161-windows-x64.exe**).

14. Follow the steps to install Java Run Time.

15. To install **ZAP** navigate to **Z:\CEH-Tools\CEHv10 Module 11 Session Hijacking\Session Hijacking Tools\OWASP ZAP**, double-click **ZAP_2_7_0_windows.exe**, and follow the installation steps to install.

16. Once installation is complete, launch **ZAP** from **Start** menu **apps** or double-click **ZAP2.7.0** on the Desktop.

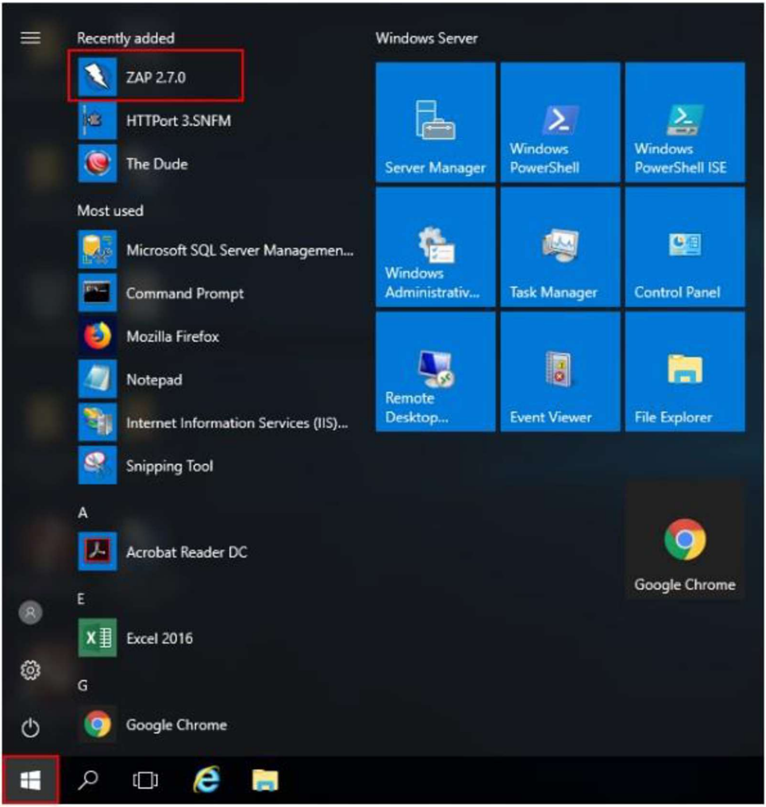
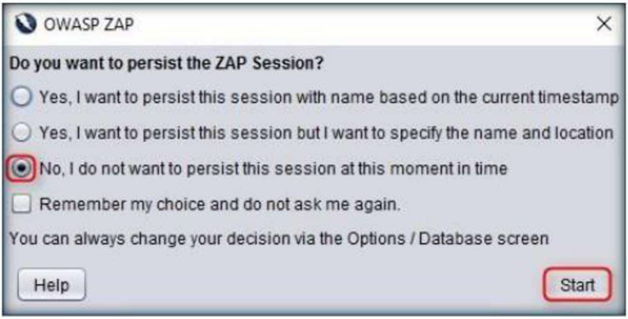


FIGURE 1.7: Windows Server 2016 Apps list

17. If **ZAP: Licensed under the Apache License** wizard appears, read the following agreement, and click **Accept** to accept the terms and conditions of the OWASP ZAP.

18. If the **ZAP Tips and Tricks** wizard appears; once the process is completed, it closes.

19. A prompt that reads **Do you want to persist the ZAP Session?** is displayed. Select **No, I do not want to persist this session at this moment in time**, and click **Start**.



Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

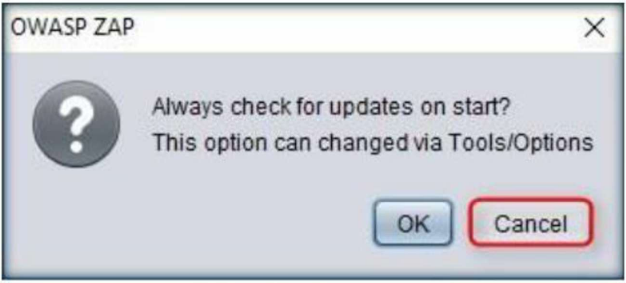
● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

FIGURE 1.8: OWASP ZAP Persist Session

20. If **Always check for updates on start** pop-up appears, click **Cancel** as shown in the screenshot.



Always check for updates on start?
This option can changed via Tools/Options

FIGURE 1.9: OWASP ZAP Persist Session

21. The **OWASP ZAP** main window appears; click on the "**+**" icon in the right pane, as shown in the figure below to add the **Break** tab.

22. The **Break** tab allows you to **modify** a response or request when it has been caught by the ZAP.

23. It also allows you to modify some elements that you cannot modify through your browser; these include:

    a) The header

    b) Hidden fields

    c) Disabled fields

    d) Fields that use **JavaScript** to filter out illegal characters

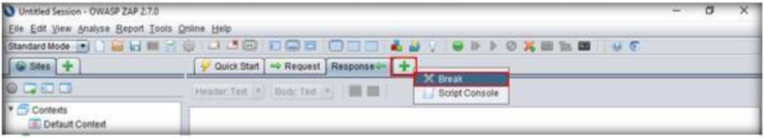


FIGURE 1.10: OWASP ZAP Persist Session

24. Once the **Break** tab is added in your OWASP ZAP window, configure the ZAP to work as a proxy.

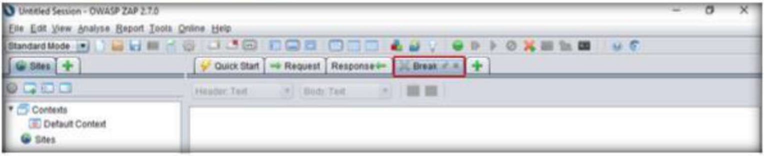


FIGURE 1.11: OWASP ZAP Persist Session

25. To configure ZAP as a proxy, click **Settings** icon from the tool bar as shown in the following screenshot.

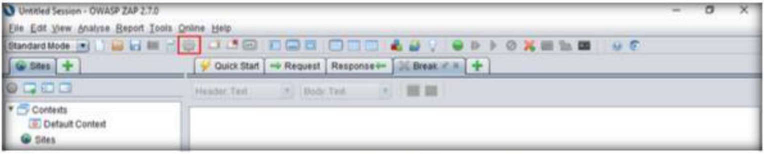
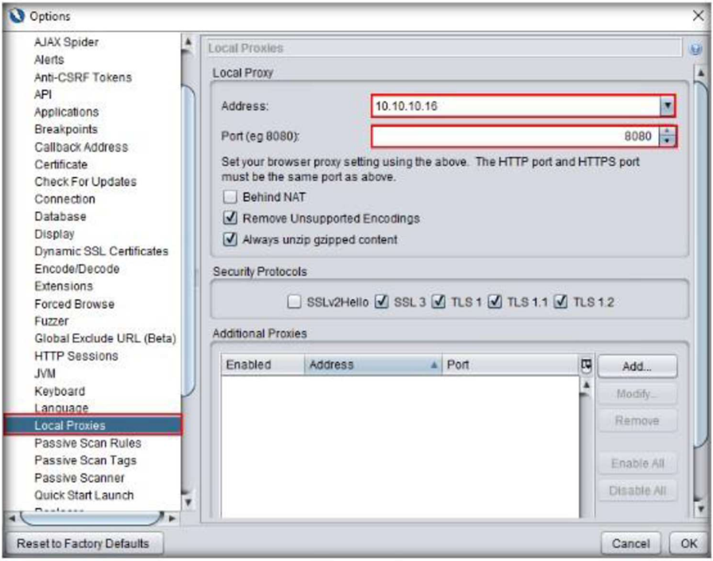


FIGURE 1.12: OWASP ZAP Persist Session

26. The **Options** window appears; select **Local Proxies** from the left pane; in the **Address** field, type the **Windows Server 2016** machine IP address, set the **Port** to default, and then click **OK**.



Local Proxies

Local Proxy

Address: 10.10.10.16

Port (eg 8080): 8080

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

☐ Behind NAT

☑ Remove Unsupported Encodings

☑ Always unzip gzipped content

Security Protocols

☐ SSLv2Hello ☑ SSL 3 ☑ TLS 1 ☑ TLS 1.1 ☑ TLS 1.2

Additional Proxies

Enabled	Address	Port

FIGURE 1.13: OWASP ZAP Persist Session

27. Click **Set break on all requests and responses**● from the tool bar of ZAP.

28. This button sets and unsets a global break point that will trap and display the next response or request in Break tab from the victims' machine.

29. You can modify any part of the request or response that you want and send it to the victim's application by clicking either **Step** or **Continue**.

30. Alternatively, you can click **Drop** to dispose of the request or response.

Note: Set break on all requests and responses turns automatically from green to red.

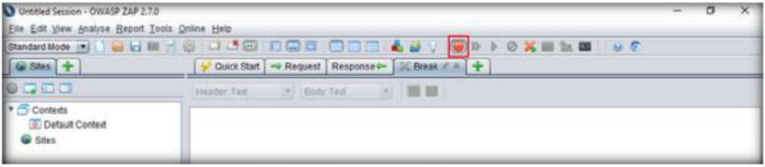


FIGURE 1.14: OWASP ZAP Persist Session

31. Now, switch back to the victim machine **Windows 10**, and launch the same browser in which you have configured the proxy settings.

32. In this lab, we have configured for Google Chrome browser.

33. Type **www.moviescope.com** in the address bar and press **Enter** as shown in the following screenshot.

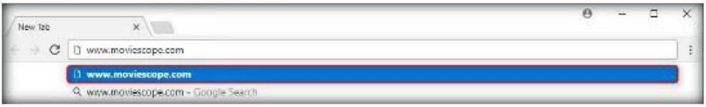
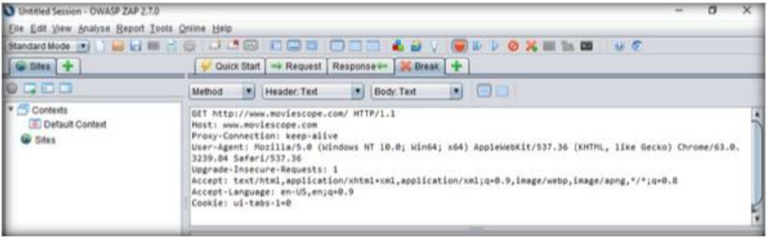


FIGURE 1.15: OWASP ZAP Persist Session

34. Now, switch to the attacker machine **Windows Server 2016**, and in a ZAP proxy, it starts capturing the requests of the victim machine.

35. Now click the ▷ button until you capture the **GET** request of the browsed website in the victim machine.

36. In this lab, we have browsed **www.moviescope.com** in the victim's machine.

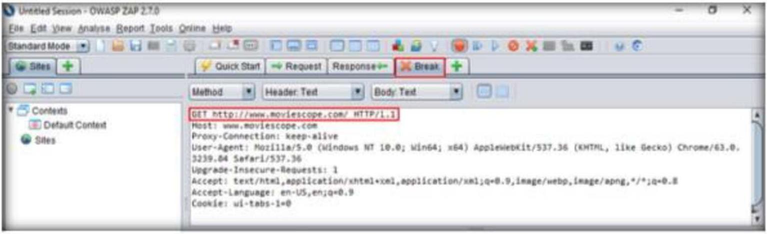


```
GET http://www.moviescope.com/ HTTP/1.1
Host: www.moviescope.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.
3239.84 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Cookie: ui-tabs-1=0
```

FIGURE 1.16: OWASP ZAP Persist Session

37. Observe the **Break** tab in the ZAP window while clicking the ▷ button to capture **www.moviescope.com**.

38. Once ZAP starts, capture the victim machine browsing traffic, as shown in the figure.



```
GET http://www.moviescope.com/ HTTP/1.1
Host: www.moviescope.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.
3239.84 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Cookie: ui-tabs-1=0
```

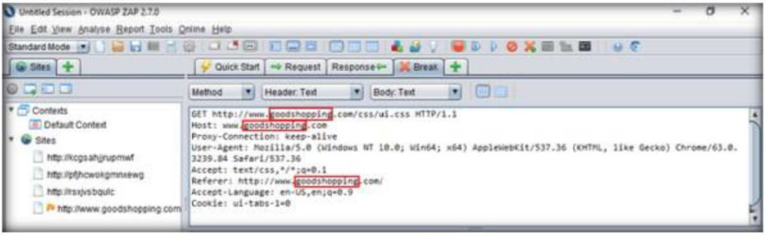
FIGURE 1.17: OWASP ZAP Persist Session

39. Now, modify **www.moviescope.com** to **www.goodshopping.com** in all the GET requests captured on the **Break** tab.

40. Once you have modified the **GET** request, click ▷ to forward traffic to the victim machine.

41. Perform this process until you see the **www.goodshopping.com** page in the victim machine.

    Note: Simultaneously, you can switch to victim's machine to see the browser status.



```
GET http://www.goodshopping.com/css/ui.css HTTP/1.1
Host: www.goodshopping.com
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.
3239.84 Safari/537.36
Accept: text/css,*/*;q=0.1
Referer: http://www.goodshopping.com/
Accept-Language: en-US,en;q=0.9
Cookie: ui-tabs-1=0
```

FIGURE 1.18: OWASP ZAP Persist Session

42. Now, switch to victim's machine (**Windows 10**); the browser displays the other website the attacker wants to see in the victim's machine.

43. Actually, the victim has browsed **www.moviescope.com** but now sees **www.goodshopping.com**.

44. The address bar displays **www.moviescope.com** but the window displays **www.goodshopping.com**.

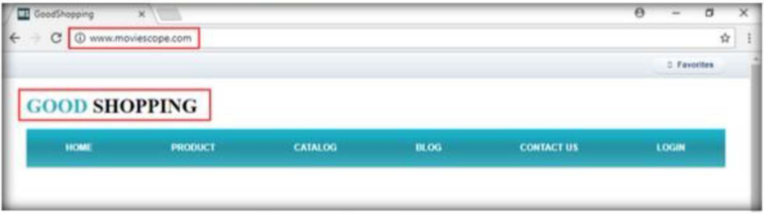


FIGURE 1.18: OWASP ZAP Persist Session

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ **Yes**	☑ **No**
Platform Supported	
☑ **Classroom**	☑ **iLabs**

Lab

2

Perform sslstrip and Intercept HTTP Traffic through BetterCAP

BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real time, sniff for credentials and much more.

Lab Scenario

Attackers can use session hijacking to launch various kinds of attacks, such as man-in-the middle (MITM) attack. An MITM attack is one in which the attacker places himself between the client and server. Session hijacking enables the attackers to place themselves between the authorized client and the web server, so that all information—traveling in either direction—must pass through them.

An ethical hacker or a penetration tester, you must know the working of an MITM attack to protect your organization's sensitive information from the attack.

Lab Objectives

The objective of this lab is to learn how to:

- Intercept Traffic and sniff out user credentials from a network

Lab Environment

In this lab, you will need:

- A computer running Windows Server 2016
- A computer running Kali Linux on virtual machine as Attacker Machine
- A web browser with Internet access
- Administrative privileges to run this tool

Lab Duration

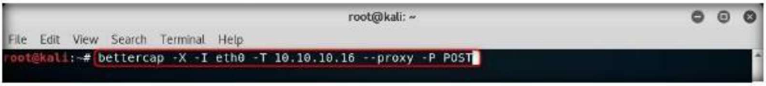
Time: 5 Minutes

Overview of Lab

This lab will demonstrate how to intercept the traffic of the victim's machine by using a proxy and also how to view all the POST activity to sniff out user's login credentials.

Lab Tasks

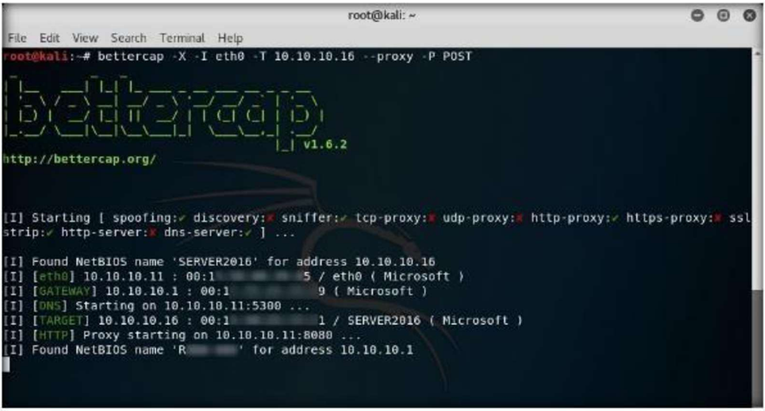
1. Log-in to **Kali Linux** machine and open a terminal window.
2. In the terminal window, type **bettercap -X -I eth0 -T 10.10.10.16 --proxy -P POST** and hit **Enter**.



```
root@kali:~# bettercap -X -I eth0 -T 10.10.10.16 --proxy -P POST
```

FIGURE 2.1: Bettercap script to intercept traffic

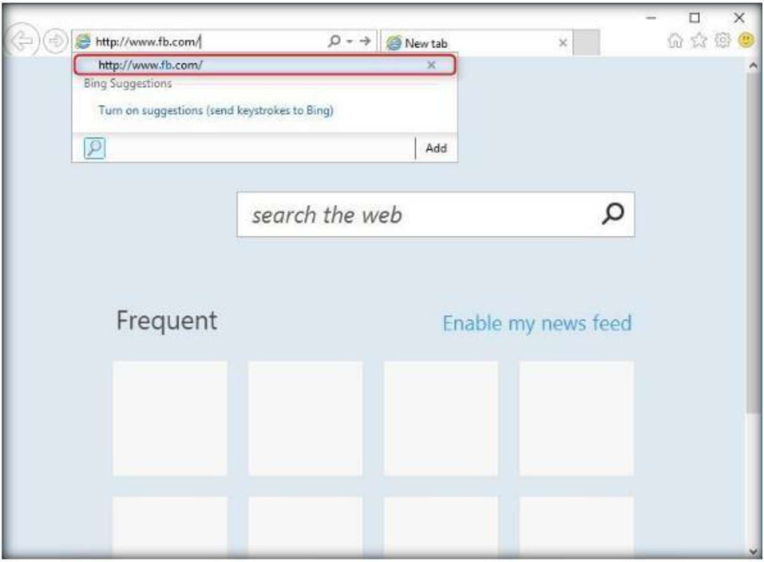
3. Bettercap starts to listen the POST activity on the **Windows Server 2016** system as shown in the screenshot.



```
root@kali:~# bettercap -X -I eth0 -T 10.10.10.16 --proxy -P POST

                          |_| v1.6.2
http://bettercap.org/


[I] Starting [ spoofing:✓ discovery:✗ sniffer:✓ tcp-proxy:✗ udp-proxy:✗ http-proxy:✓ https-proxy:✗ ssl
strip:✓ http-server:✗ dns-server:✓ ] ...

[I] Found NetBIOS name 'SERVER2016' for address 10.10.10.16
[I] [eth0] 10.10.10.11 : 00:1[redacted]5 / eth0 ( Microsoft )
[I] [GATEWAY] 10.10.10.1 : 00:1[redacted]9 ( Microsoft )
[I] [DNS] Starting on 10.10.10.11:5300 ...
[I] [TARGET] 10.10.10.16 : 00:1[redacted]1 / SERVER2016 ( Microsoft )
[I] [HTTP] Proxy starting on 10.10.10.11:8080 ...
[I] Found NetBIOS name 'R[redacted]' for address 10.10.10.1
```

FIGURE 2.2: Starting Bettercap

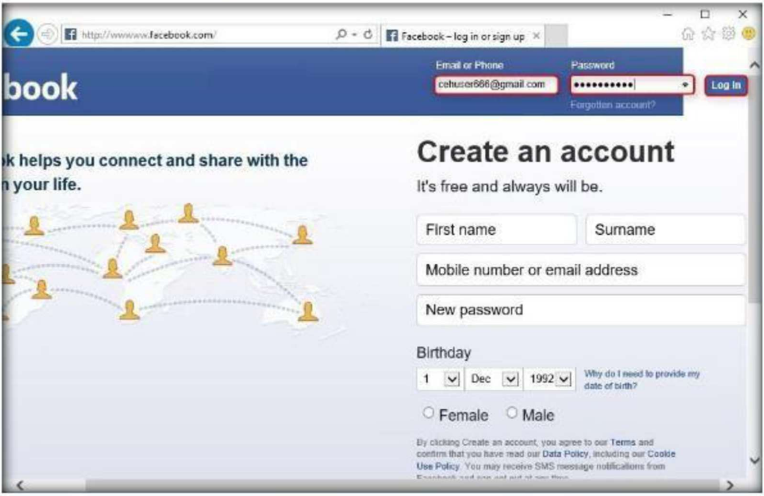
4. Now switch to the **Windows Server 2016** system and open any browser (here, Internet Explorer). In the address bar, type **http://www.fb.com** as the URL and hit **Enter**.



http://www.fb.com/

FIGURE 2.3: Opening Facebook

5. Facebook page appears, type your username-password and click **Log In**, as shown in the screenshot.



http://www.www.facebook.com/

Email or Phone: cehuser686@gmail.com

Password: ••••••••••

k helps you connect and share with the
n your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

New password

Birthday: 1 | Dec | 1992

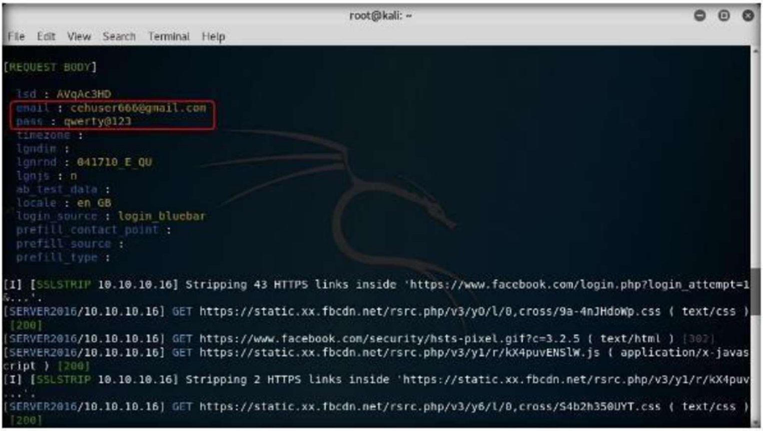
Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Create an account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from

FIGURE 2.4: Logging into Facebook

6. Now when you switch back to the **Kali Linux** machine, you will find that bettercap has sniffed the user credentials you entered and is available in plain text for the attacker to use as shown in the screenshot.



```
[REQUEST BODY]

  lsd : AVqAc3HD
  email : cehuser666@gmail.com
  pass : qwerty@123
  timezone :
  lgndim :
  lgnrnd : 041710_E_QU
  lgnjs : n
  ab_test_data :
  locale : en_GB
  login_source : login_bluebar
  prefill_contact_point :
  prefill_source :
  prefill_type :

[I] [SSLSTRIP 10.10.10.16] Stripping 43 HTTPS links inside 'https://www.facebook.com/login.php?login_attempt=1
&...'.
[SERVER2016/10.10.10.16] GET https://static.xx.fbcdn.net/rsrc.php/v3/yO/l/0,cross/9a-4nJHdoWp.css ( text/css )
 [200]
[SERVER2016/10.10.10.16] GET https://www.facebook.com/security/hsts-pixel.gif?c=3.2.5 ( text/html ) [302]
[SERVER2016/10.10.10.16] GET https://static.xx.fbcdn.net/rsrc.php/v3/y1/r/kX4puvENSlW.js ( application/x-javas
cript ) [200]
[I] [SSLSTRIP 10.10.10.16] Stripping 2 HTTPS links inside 'https://static.xx.fbcdn.net/rsrc.php/v3/y1/r/kX4puv
...'.
[SERVER2016/10.10.10.16] GET https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0,cross/S4b2h350UYT.css ( text/css )
 [200]
```

FIGURE 2.5: User credentials obtained through Bettercap

Lab Analysis

Analyze and document the results related to this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ **Yes**	□ **No**
Platform Supported	
☑ **Classroom**	□ **iLabs**