Session Hijacking

Module 10

Hijacking Sessions

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

ICON KEY
Valuable information
Test your knowledge
Web exercise
Workbook review

Lab Scenario

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

According to KrebsonSecurity news and investigation, zero-day vulnerability in yahoo.com that lets attackers 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 lets attackers 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, and can 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 messages that you were not expecting.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 10 Session Hijacking

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 provides 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
- Perform ARP Poisoning using Cain & Abel
- Modify Cookies and Hijack a session using Firebug

Lab Environment

To carry out this, you need:

- A computer running Windows Server 2012 as host machine
- Kali Linux virtual machine
- Windows 8.1 virtual machine
- Web browser with Internet access
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 65 Minutes

Overview of Session Hijacking

TASK 1

Overview

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. Because 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)
- Hijacking a User Session Using **Firebug**
- Hijacking **HTTPS** Traffic in a Network Using **sslstrip**
- Performing a **MITM** Attack and Hijacking an Established Session Using **Websploit**

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.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

ZAP is an Intercepting Proxy. It allows you to see all of the requests you make to a web app and all of 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 2012 as Attacker machine
- Windows 8.1 running on virtual machine as a Target machine
- Owasp-ZAP located at **D:\CEH-Tools\CEHv9 Module 10 Session Hijacking\Session Hijacking Tools\Zaproxy**
- 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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 10 Session Hijacking

- Java Run Time 7 requires to run this tool, is located at **D:\CEH-Tools\CEHv9 Module 10 Session Hijacking\Session Hijacking Tools\Zaproxy**
- 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

TASK 1

Find Live Hosts

1. Before starting this lab, we need to configure the **proxy** settings in the victim's machine. In this lab **Windows 8.1** machine will be the victim machine.
2. Launch Windows 8.1 virtual machine, **log in**, 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.

ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

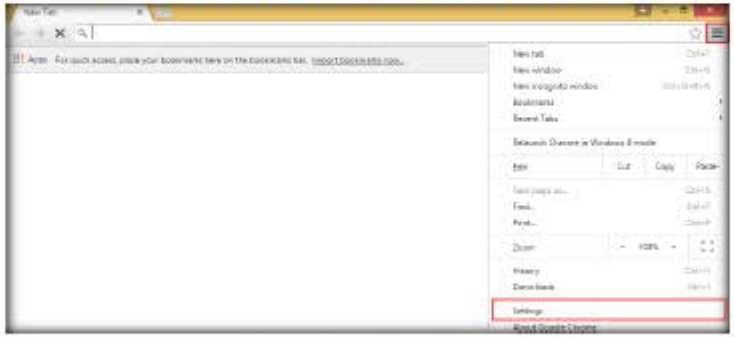


FIGURE 1.1: Google Chrome Settings

4. The **Chrome://settings** window opens; scroll down to click **Show advanced settings** in the browser.

ZAP is an Interorpting Proxy. It allows you to see all of the requests you make to a web app and all of the responses you receive from it. Amongst other things this allows you to see AJAX calls that may not otherwise be obvious.

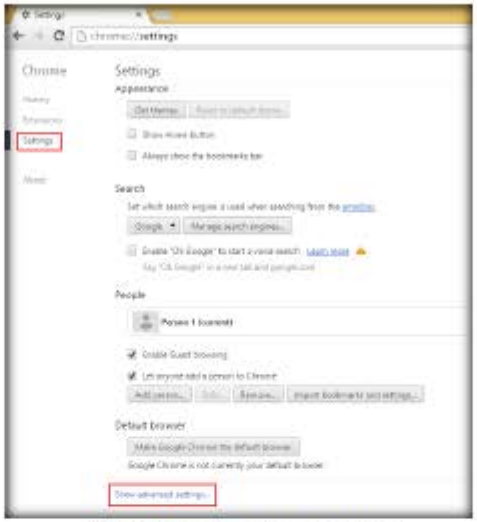


FIGURE 1.2: Google Chrome Show advanced settings

5. In the **Network** section, click **Change proxy settings...** to configure a proxy.

Active scanning attempts to find potential vulnerabilities by using known attacks against the selected targets.

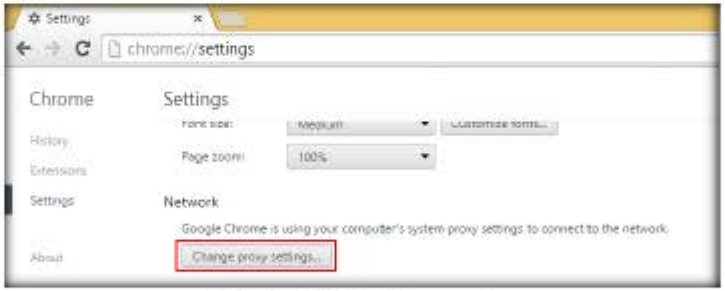


FIGURE 1.3: Google Chrome Change proxy settings

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

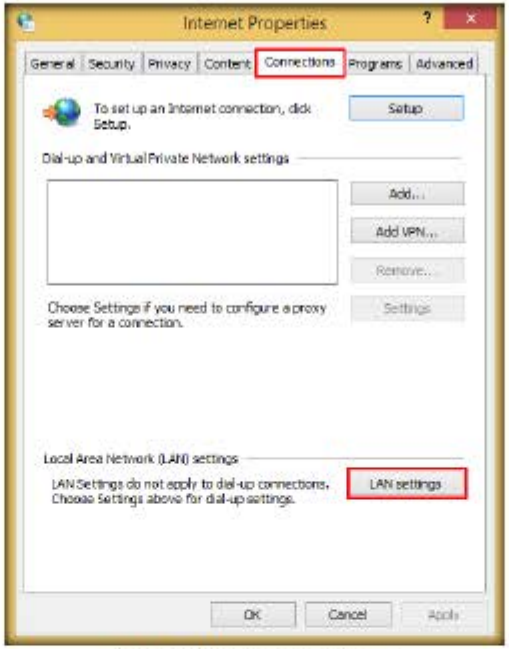


FIGURE 1.4: LAN Settings in Internet Properties

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**.

Active scanning is an attack on those targets. You should NOT use it on web applications that you do not own.

It should be noted that active scanning can only find certain types of vulnerabilities. Logical vulnerabilities, such as broken access control, will not be found by any active or automated vulnerability scanning.

Manual penetration testing should always be performed in addition to active scanning to find all types of vulnerabilities.

9. In this lab, the attacker machine would be **Windows Server 2012;** its IP address is **10.0.0.5**.

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

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**.

This will exclude the selected nodes from the proxy. They will still be proxied via ZAP but will not be shown in any of the tabs.

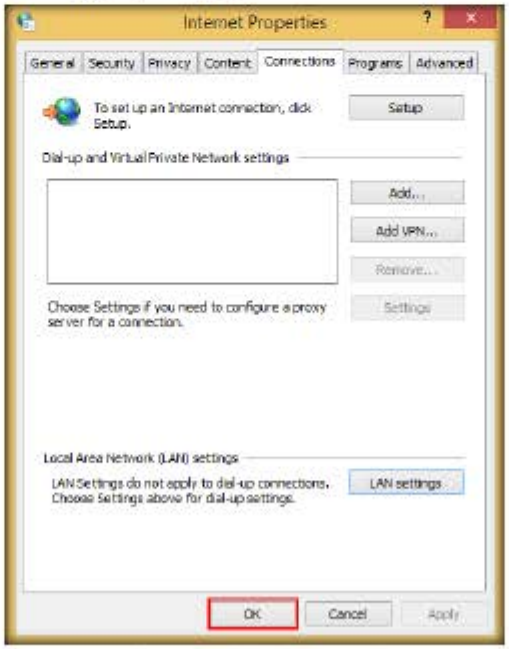


FIGURE 1.6: LAN Settings in Internet Properties

11. Now you have configured victim machine proxy settings. Close the browser.
12. Switch to **Windows Server 2012** attacker machine, and install OWASP-ZAP (Zed Attack Proxy).
13. Prior to installation, ZAP make sure that **Java Run Time 7** is installed in your attacker machine (if not, you can navigate to **D:\CEH-Tools\CEHv9 Module 10 Session Hijacking\Session Hijacking Tools\Zaproxy** and double-click **jre-7-windows-x64.exe**).
14. Follow the steps to install Java Run Time.
15. To install **ZAP** navigate to **D:\CEH-Tools\CEHv9 Module 10 Session Hijacking\Session Hijacking Tools\Zaproxy**, double-click **ZAP_2.4.0_Windows.exe,** and follow the installation steps to install.

Request tab: This shows the data your browser sends to the application

16. Once installation is complete, launch **ZAP** from Start menu apps, or double-click **OWASP ZAP 2.4.0** on the desktop.

FIGURE 1.7: Windows Server 2012 Apps Screen

17. ZAP: Licensed under the Apache License, Version 2.0. wizard appears, read the following agreement, and click **Accept** to accept the terms and conditions of the OWASP ZAP.

Response tab: This shows the data the application sends back to your browser.

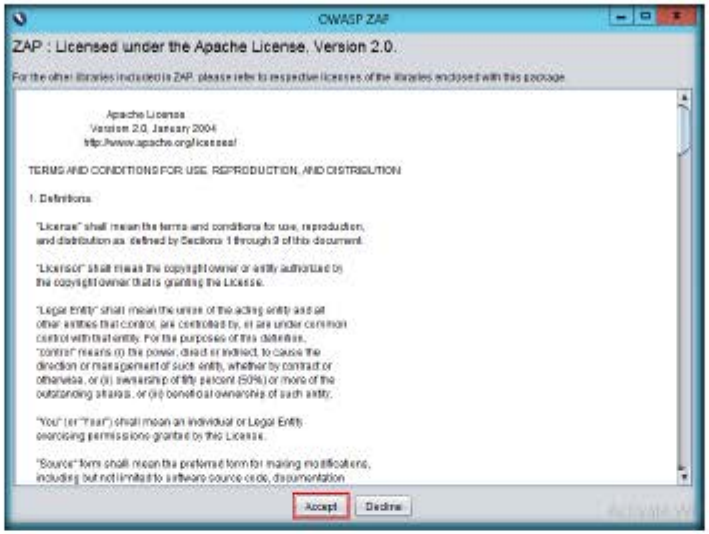


FIGURE 1.8: OWASP ZAP License Agreement

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

Break tab: This allows you to manipulate the data.

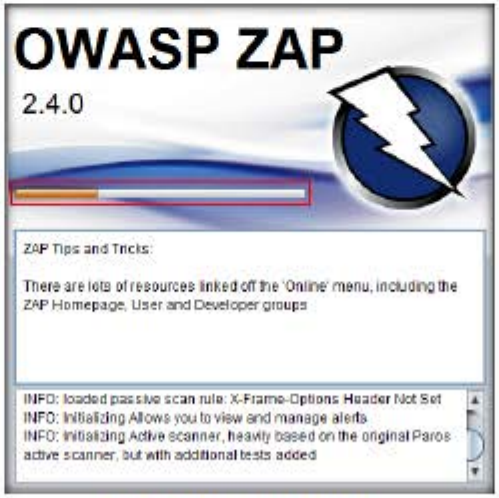


FIGURE 1.9: OWASP ZAP TIPS and Tricks

History tab: This shows the requests in the order they were made.

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**.

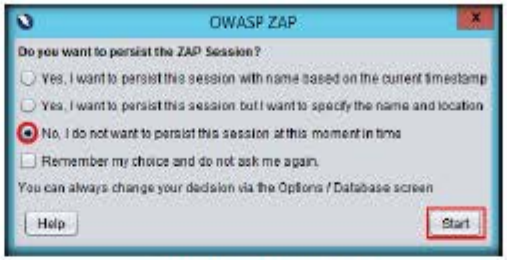


FIGURE 1.10: OWASP ZAP Persist Session

20. 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.
21. The **Break** tab allows you to **modify** a response or request when it has been caught by the ZAP.
22. 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 1.11: OWASP ZAP Persist Session

While the Break tab is not in use its icon is a grey cross: ✖
When a break point is hit the tab icon is changed to a red cross: ✖

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

FIGURE 1.12: OWASP ZAP Persist Session

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

Search tab: This allows you to search all of the requests and responses.

FIGURE 1.13: OWASP ZAP Persist Session

25. The Options window appears; select **Local proxy** from the left pane; and in the **Address** field, type the Windows Server 2012 machine IP address, set the Port to default, and then click **OK**.

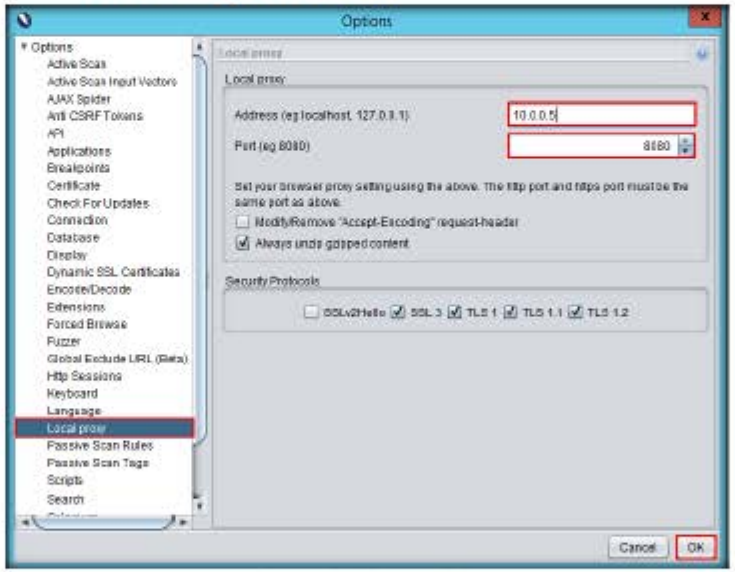


FIGURE 1.14: OWASP ZAP Persist Session

The Options Connection screen allows you to configure the address and port on which ZAP accepts incoming connections.
It is this address and port that you must configure your browser to use as a proxy.

26. Click **Set break on all requests and responses** from the tool bar of ZAP.
27. This button sets and unsets a global break point that will trap and display from the victims machine the next response or request in Break tab.
28. 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**.
29. 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.

This changes the display so that the 'tree' window containing the Sites tab extends for the full length of the left hand side. This will reduce the amount of space available to the 'information' window.

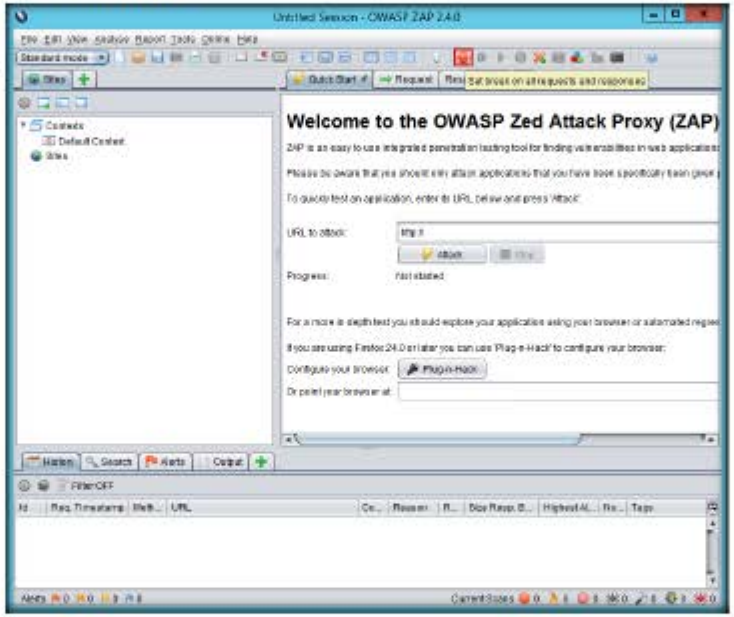


FIGURE 1.15: OWASP ZAP Persist Session

This sets and unsets a 'global' break point that will trap and display the next response in the Break tab. You can then change any part of the response that you want to and send it to your browser by pressing either of the 'Step' or 'Continue' buttons. Alternatively you can press the 'Drop' button to dispose of the request. You can switch between a single 'combined' break button and separates ones for requests and responses via the Options breakpoints screen.

30. Now, switch back to the victim machine Windows 8.1, and launch the same browser in which you have configured the proxy settings.
31. In this lab, we have configured for Google Chrome browser.
32. Type www.moviescope.com in the address bar, and press **Enter** as shown in the following screenshot.

FIGURE 1.16: OWASP ZAP Persist Session

33. Now, switch to the Attacker machine Windows Server 2012, and in a ZAP proxy, it starts capturing the requests of the victim machine.
34. Now click the button until you capture the **GET** request of the browsed website in the victim machine.
35. In this lab, we have browsed www.moviescope.com in the victim's machine.

This allows the trapped request or response to continue to the application or your browser with any changes that you have made to it. The 'global' break point will remain set so that the next request or response will also be caught. This button is only enabled when a request or response is trapped.

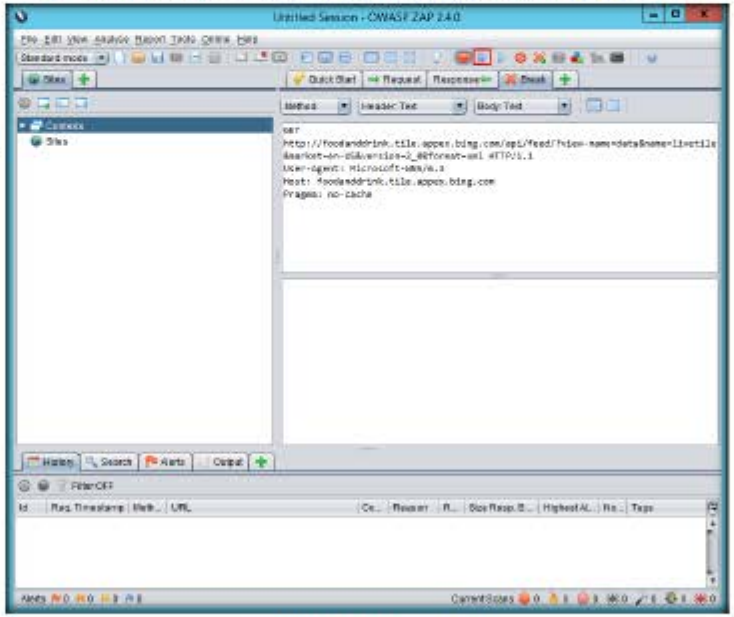


FIGURE 1.17: OWASP ZAP Persist Session

36. Observe the Break tab in the ZAP window while clicking the button to capture www.moviescope.com.
37. Once ZAP starts, capture the victim machine browsing traffic, as shown in the figure.

The 'global' break point will be unset so that subsequent requests and responses will no longer be caught by ZAP unless you have set break points on specific URLs.
This button is only enabled when a request or response is trapped.

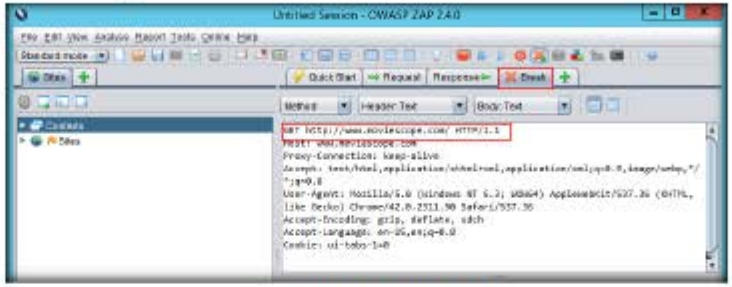


FIGURE 1.18: OWASP ZAP Persist Session

38. Now, modify www.moviescope.com to www.goodshopping.com in all the GET requests captured on the **Break** tab.
39. Once you have modified the **GET** request, click to forward traffic to the victim machine.
40. 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.

Manage Add-ons dialog which allows you to discover, install and update add-ons from the online marketplace.
It also allows you to uninstall add-ons.

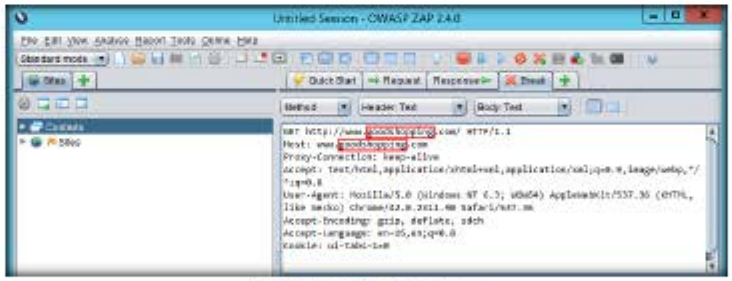


FIGURE 1.19: OWASP ZAP Persist Session

41. Now, switch to Victim's machine; the browser displays the other website the attacker wants to see in the victim's machine.
42. Actually, the victim has browsed www.moviescope.com but now sees www.goodshopping.com.
43. The address bar displays www.moviescope.com but the window displays www.goodshopping.com.

Footer displays counts of the High, Medium, Low and Informational alerts and counts of the currently active and spider scans. It can also contain counters of scanners provided by add-ons.

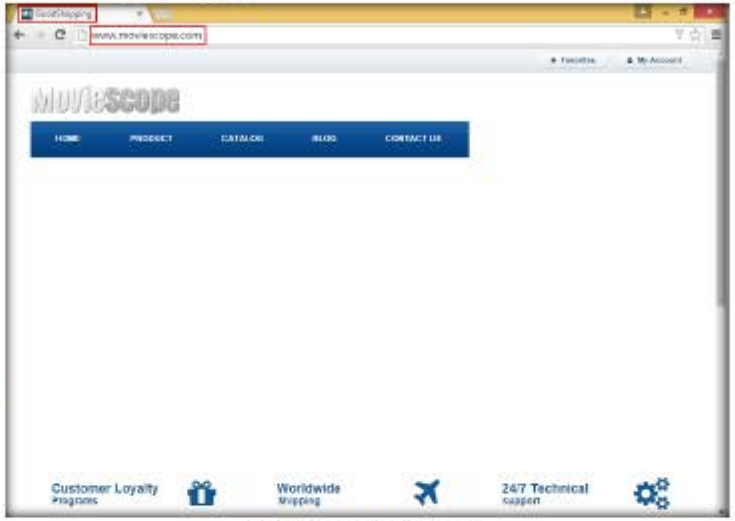


FIGURE 1.20: OWASP ZAP Persist Session

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

Hijacking a User Session with Firebug

Firebug allows viewing and managing cookies in your browser. You can deny cookies for specific sites, filter cookies, create new and delete existing cookies.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers are continuously watching for websites to hack, so developers must be prepared to counterattack malicious hackers by writing strong, secure codes. A common form of attack is session hijacking (i.e., accessing a website using someone else's session ID). A session ID might contain credit card details, passwords, and other sensitive information that can be misused by a hacker.

Session hijacking attacks are performed either by session ID guessing or by stolen session ID cookies. Session ID guessing involves gathering a sample of session IDs and "guessing" a valid session ID assigned to someone else. It is always recommended not to replace ASP.NET session IDs with those of your own, as this will prevent session ID guessing. Such session hijacking attacks can be prevented by using SSL; however, attackers can steal session ID cookies using cross-site scripting attacks and other methods. If an attacker gets hold of a valid session ID, then ASP.NET connects to the corresponding session with no further authentication.

There are many tools easily available now that attackers use to hack into websites or user data, one of which is Firesheep, a Firefox add-on. Although you are connected to an unsecure wireless network, this Firefox add-on can sniff the network traffic and capture all your information and provide it to the hacker in the same network. The attacker can now use this information and login as you.

As an Ethical Hacker, Penetration Tester, or Security Administrator, you should be familiar with network and web authentication mechanisms. In your role of web security administrator, you need to test web server traffic for weak session IDs, insecure handling, identity theft, and information loss. Always ensure that you have an encrypted connection using https, which will make the sniffing of network packets difficult for an attacker. Alternatively, VPN connections can also be used to stay safe and

advise users to log off once they are done with their work. In this lab, you will learn to use Firebug to intercept a session and gain unauthorized access to the victim's session.

Lab Objectives

The objective of this lab is to help students learn session hijacking and how to take necessary actions to defend against session hijacking.

In this lab, you will:

- Intercept and modify web traffic
- Attain a user session without specifying the login credentials

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 10 Session Hijacking

Lab Environment

To carry out the lab, you need:

- Firebug installed in Windows Server 2012 Host Machine
- Cain & Abel located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\ARP Poisoning Tools\Cain and Abel**
- Wireshark located at **D:\CEH-Tools\CEHv9 Module 07 Sniffing\Sniffing Tools\Wireshark**
- A system running Windows Server 2012 Host Machine having web browser with Internet access
- A Windows 8.1 virtual machine having web browser with Internet access
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 20 Minutes

Overview of Firebug

Firebug allows you to edit, debug, and monitor CSS, HTML, and JavaScript live in any web page. Firebug allows viewing and managing cookies in your browser. You can deny cookie access to specific sites, and filter, create, and delete cookies. You can also break into the debugger when specific cookies change their value, and view the line of script that causes the change.

Lab Tasks

TASK 1

Perform ARP Poisoning

1. In this lab, you will be using Cain & Abel to perform ARP poisoning on a network, and Wireshark to capture packets and obtain the target packet's cookie value.
2. Follow the installation steps to install Wireshark and Cain & Abel. If you have already installed them, skip to next step.
3. Launch the **Cain & Abel** application from the **Apps** screen.

4. The Main Window of Cain & Abel appears, as shown in the screenshot:

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

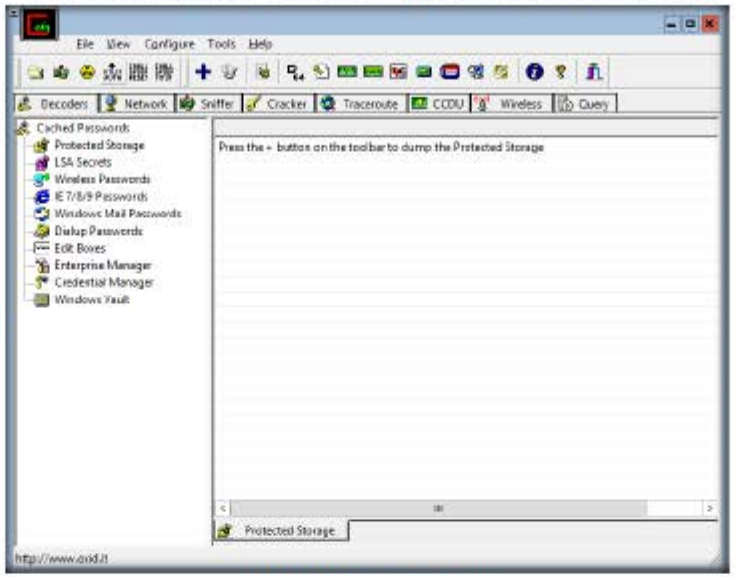


FIGURE 2.1: Cain & Abel Main Window

5. To configure **Ethernet card**, click **Configure** in the menu bar.

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

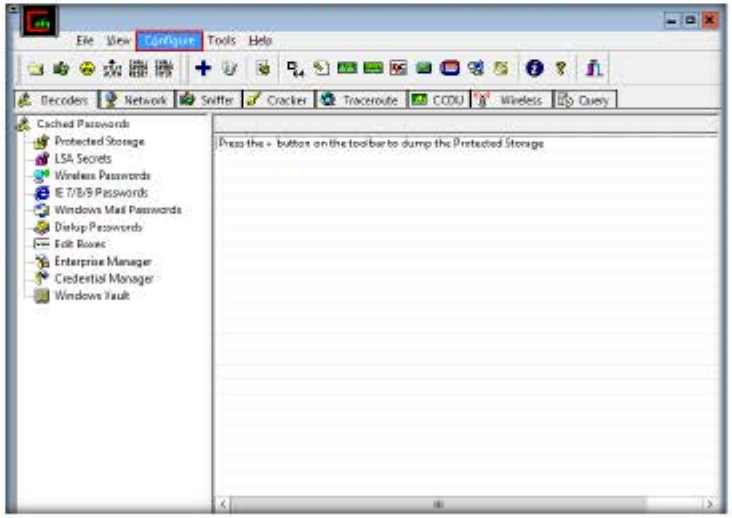


FIGURE 2.2: Cain & Abel Configuration Option

6. The **Configuration Dialog** window appears.
7. The window consists of several tabs. Click **Sniffer** tab to select sniffing adapter.
8. Select the **Adapter** associated with the IP address of the machine, click **Apply,** and then click **OK**.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.

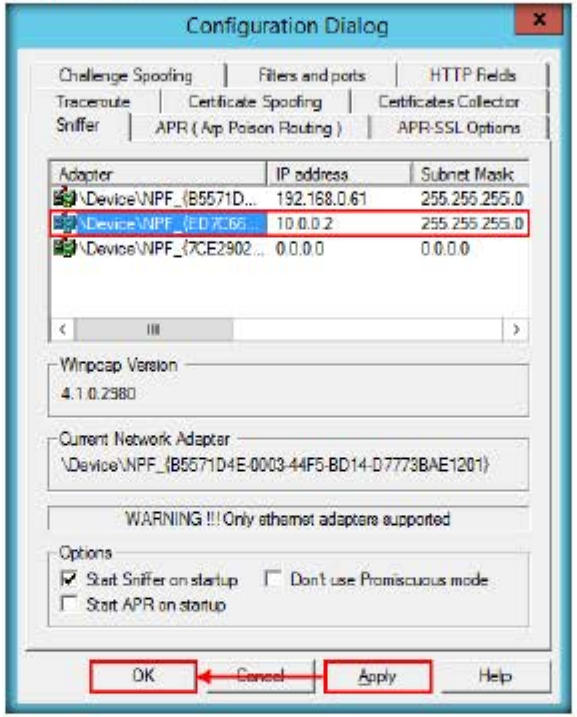


FIGURE 2.3: Cain & Abel Configuration Dialog Window

Note: If the adapter pertaining to your IP address is not listed, go to Control Panel → All Control Panel Items → Network and Sharing Center, click **Change adapter settings** link, right-click on the network adapter associated with the host machine and select **Properties**. In the Properties window, select **Internet Protocol Version 4** (TCP/IPv4), and click **Properties** button. In the IPv4 Properties window, select **General** tab, and click **Obtain an IP address automatically** radio button. Click **OK** in the **IPv4 properties** window, and click **Close** in the **Ethernet adapter properties** window.

9. Click **Start/Stop Sniffer** icon on the toolbar.

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved to a text file. APR-HTTPS can intercept and forge digital certificates on the fly but because trusted authority does not sign these certificates a warning message will be displayed to the end user.

FIGURE 2.4: Cain & Abel Configuration Dialog Window

Note: If the **Cain** warning pop-up displays, click **OK** button.

Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data.

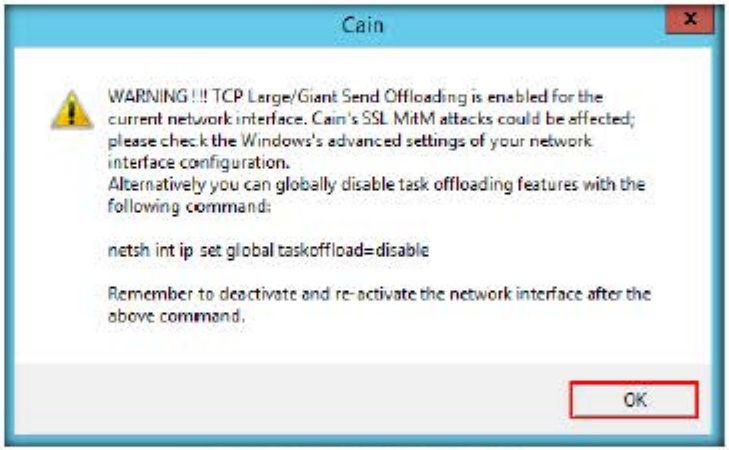


FIGURE 2.5: Cain & Abel Configuration Dialog Window

10. Now click the **Sniffer** tab.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).

FIGURE 2.6: Selecting Sniffer tab

11. Click the **+** icon; or right-click in the window, and select **Scan MAC Addresses** to scan the network for hosts.
12. The **MAC Address Scanner** window appears. Check **All hosts in my subnet,** and check the box **All Tests**. Click **OK.**

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

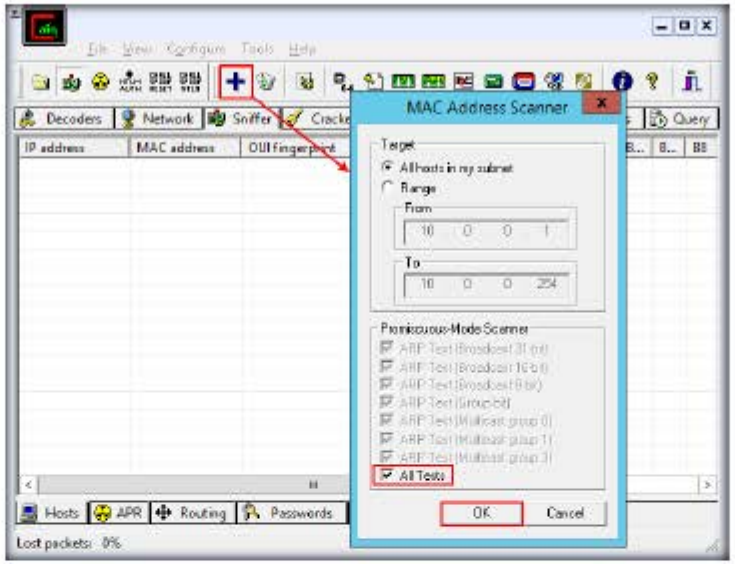


FIGURE 2.7: MAC Address Scanner window

13. Cain & Abel starts **scanning** for MAC addresses and **lists** all found MAC address.
14. After scanning is **completed**, a list of detected **MAC addresses** are displayed, as shown in the screenshots:

Speeding up packet capture speed by wireless packet injection.

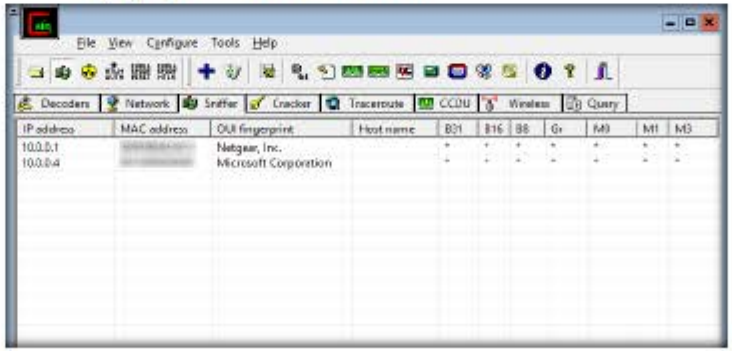


FIGURE 2.8: Scanned MAC Addresses

15. Click the **APR** tab at the bottom of the main window.

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all packets of an entire direction so it cannot grab authentications that use a challenge-response mechanism.

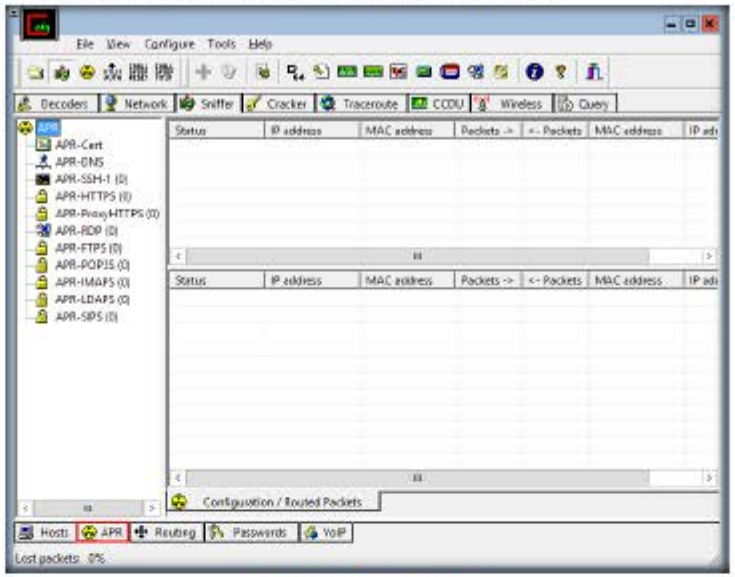


FIGURE 2.9: Choosing APR tab

16. Click anywhere on the topmost section of the right pane to activate the + icon.

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.

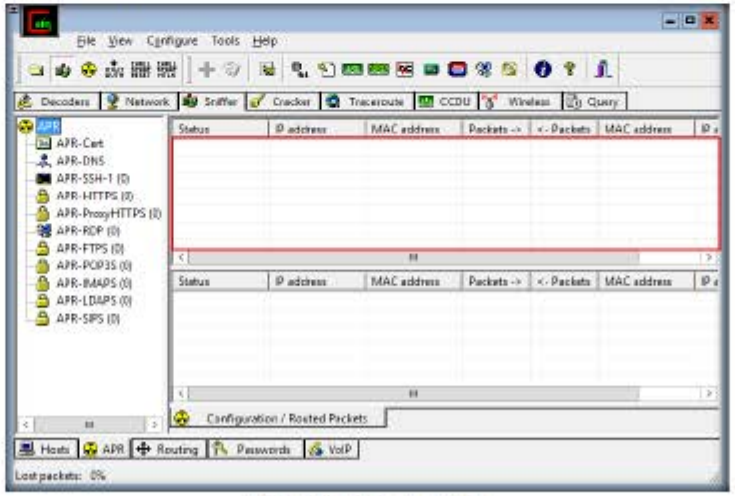


FIGURE 2.10: Activating the sniffer tab

17. Click **+**. The **New ARP Poison Routing** window opens, where we can add the IPs to listen for traffic.

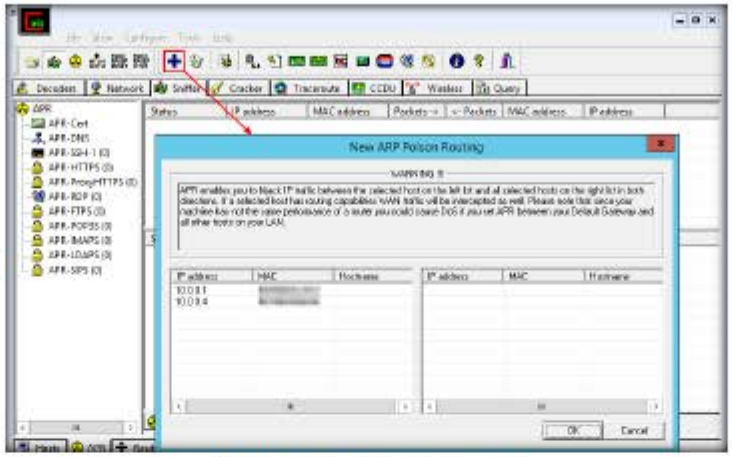


FIGURE 2.11: New ARP Poison Routing window

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primarily use is to securely store private keys that have been issued to a user.

18. Now, choose the target that you want to ARP poison in the network. In this lab, **Windows 8.1** virtual machine is the target, so, map the IP address of Windows 8.1 and default gateway, so that whatever packets traverse between these two IP addresses, that packets are ARP poisoned by Cain & Abel.

Note: In this lab, the IP address of **Windows 8.1** machine is **10.0.0.4** and the IP address of **default gateway** of the router is **10.0.0.1**. These IP addresses might vary in your lab environment.

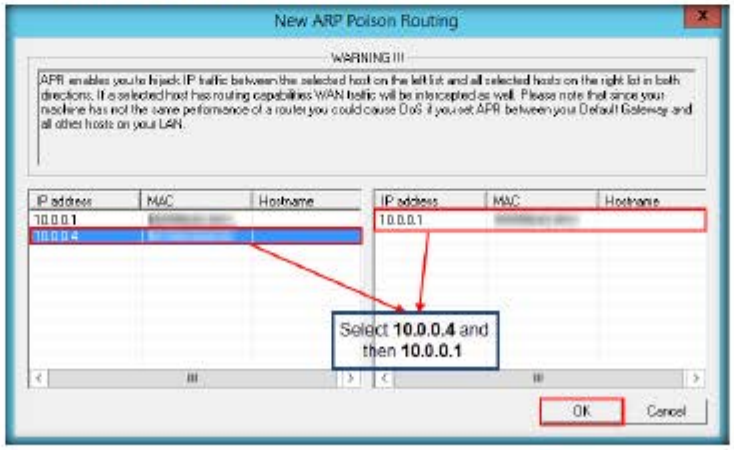


FIGURE 2.12: New ARP Poison Routing window

All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

19. Select the added IP address in the **Configuration/Routed packets** section, and click **Start/Stop APR**.

Note: If the **Couldn't bind HTTPS acceptor socket** pop-up appears, click **OK**.

Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

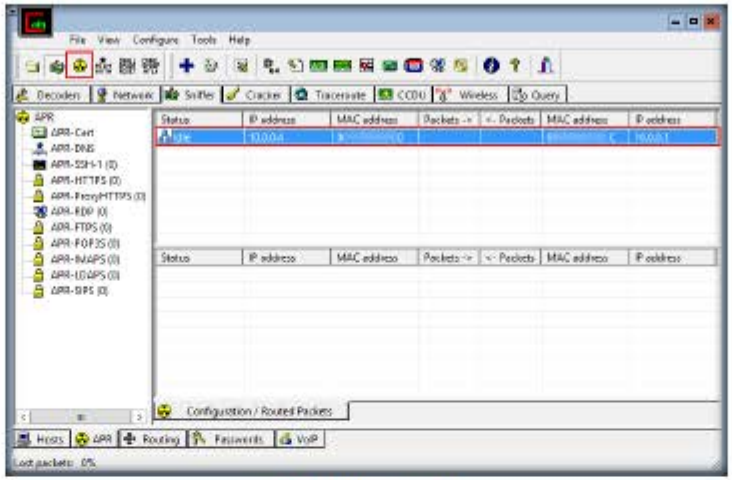


FIGURE 2.13: Starting the APR

20. As soon as you click **Start/Stop APR**, the status changes from Idle to Poisoning, and Cain & Abel begins to run ARP Poisoning:

Note that Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

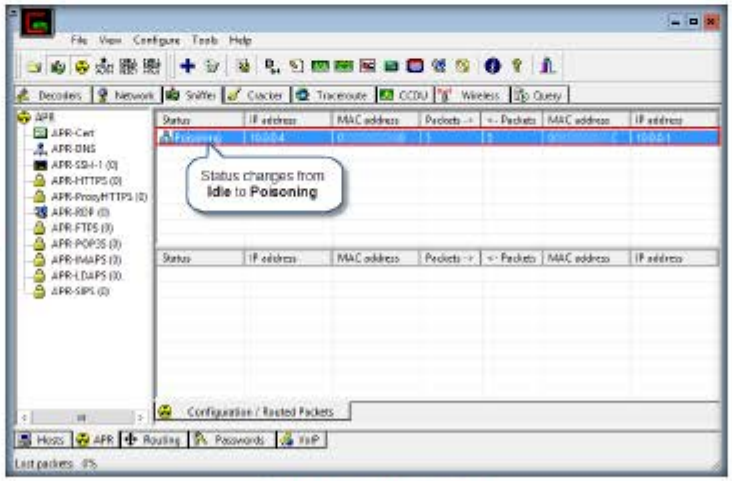


FIGURE 2.14: ARP Poisoning initiated

TASK 2

Capture Traffic Using Wireshark

21. Now, minimize the window, and launch **Wireshark** from the **Apps** screen.

22. The **Wireshark** main window appears, as shown in the screenshot:

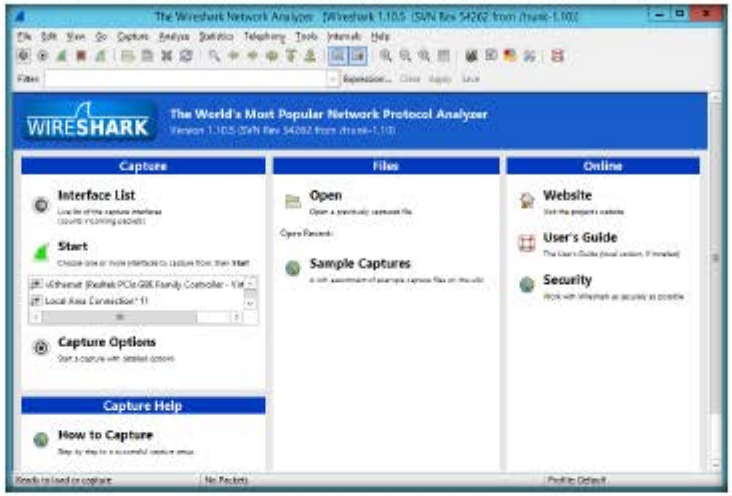


FIGURE 2.15: Wireshark main window

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

23. From the Wireshark menu bar, click on **Capture → Interfaces (Ctrl+I).**

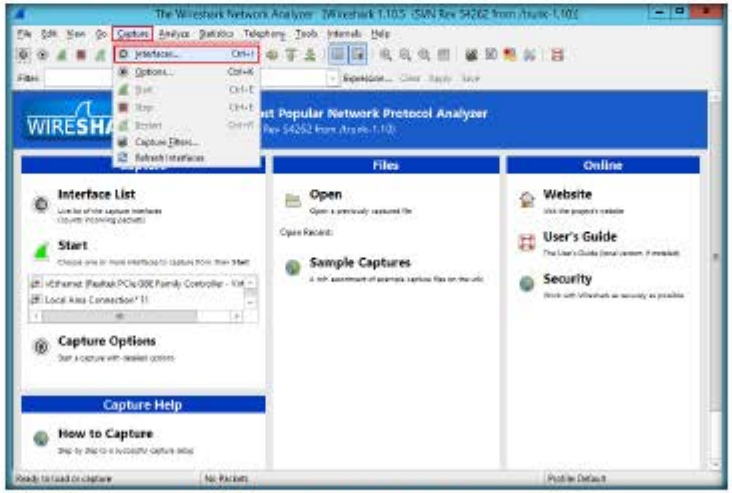


FIGURE 2.16: Wireshark Main Window with Interface Option

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

24. The **Wireshark: Capture Interfaces** window appears.

FIGURE 2.17: Wireshark Capture Interfaces Window

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well.

25. In the window, find and check the Ethernet Driver Interface that is connected to the system, as well as Hyper-V manager. In this lab, the interface is **vEthernet**.

Note: This interface might vary in your lab environment.

26. Click **Start**.

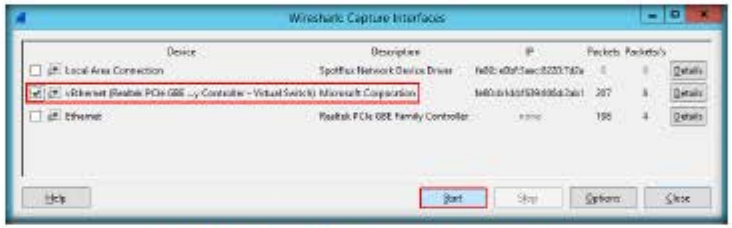
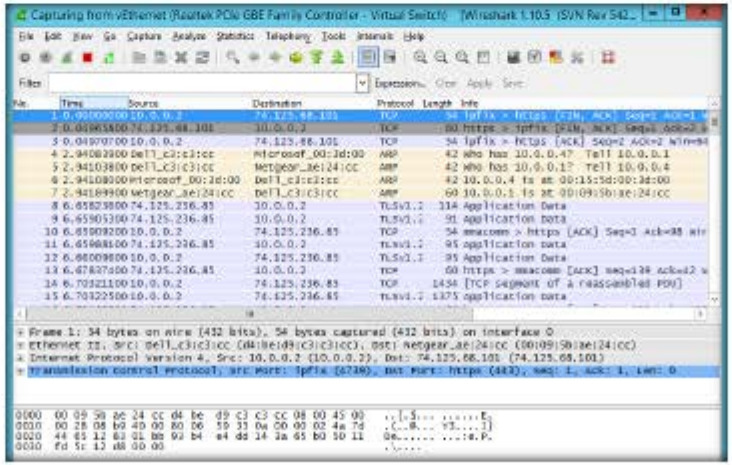


FIGURE 2.18: Wireshark Capture Interfaces Window - Starting Capture

27. Wireshark starts capturing the packets generated while traffic is received or sent from your machine.



A supported network card for capturing Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.

FIGURE 2.19: Wireshark Window Capturing the Packets

TASK 3

Log into the Goodshopping website

28. Now, log in to the **Windows 8.1** virtual machine as the victim.
29. Launch Google Chrome (or any other) web browser, type the URL http://10.0.0.2/goodshopping in the address bar, and press **Enter**.

Note: **10.0.0.2** is the IP address of the machine hosting the website (i.e., **Windows Server 2012**). Replace this IP address with that of the machine hosting the website in your lab environment.

30. The GoodShopping login/home page appears, as shown in the screenshot:

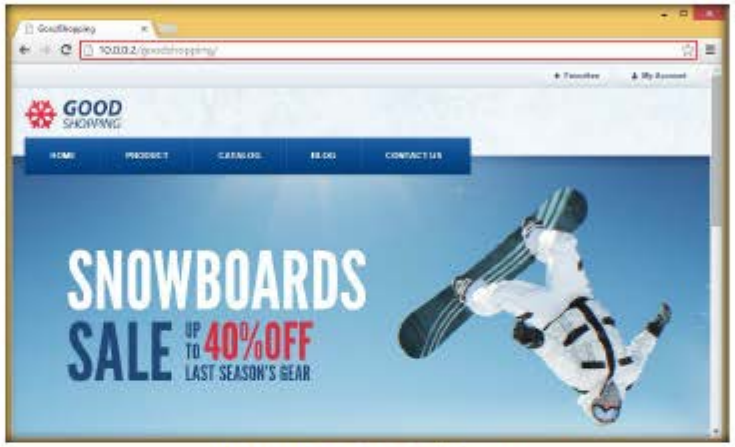


FIGURE 2.20: GoodShopping login/home page

31. Assume that you have a user account on the website.
32. Click the **My Account** tab in the top-right corner of the web page, and enter the following credentials:

    Username: **smith**

    Password: **smith123**

    Then click **Log in**.

FIGURE 2.21: Logging into GoodShopping Website

33. You are logged in successfully, as shown in the screenshot:

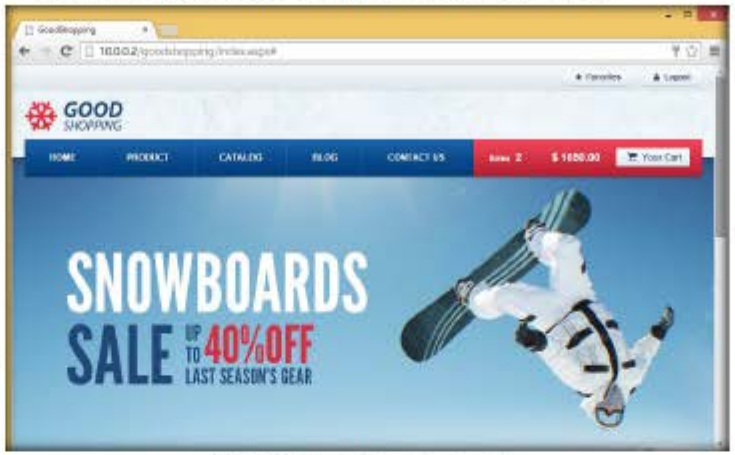


FIGURE 2.22: Successfully logged in to the website

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs

34. Now, switch back to **Windows Server 2012** host machine as the attacker, and view the **Wireshark** and **Cain & Abel** GUIs. Observe that Wireshark has captured packets and **Cain & Abel** has poisoned the routing packets.

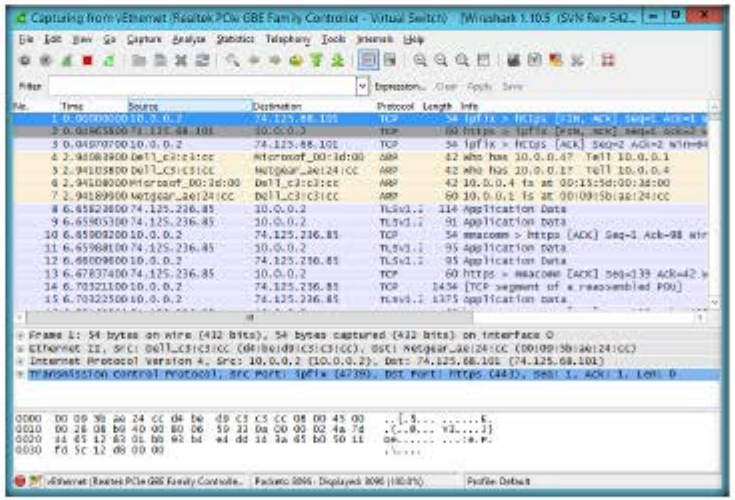


FIGURE 2.23: Wireshark capturing the packets

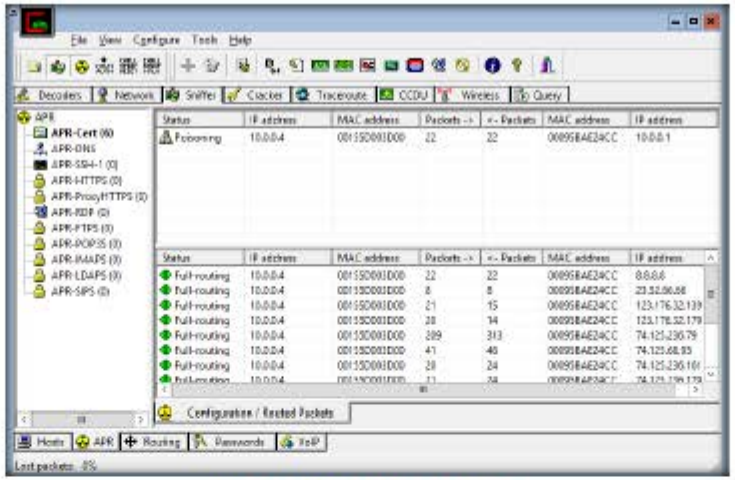


FIGURE 2.24: Cain & Abel Poisoning the Packets

TASK 4

Stop the Packet Capture and APR

35. Now, **Stop the running live capture** in Wireshark by clicking in the toolbar.

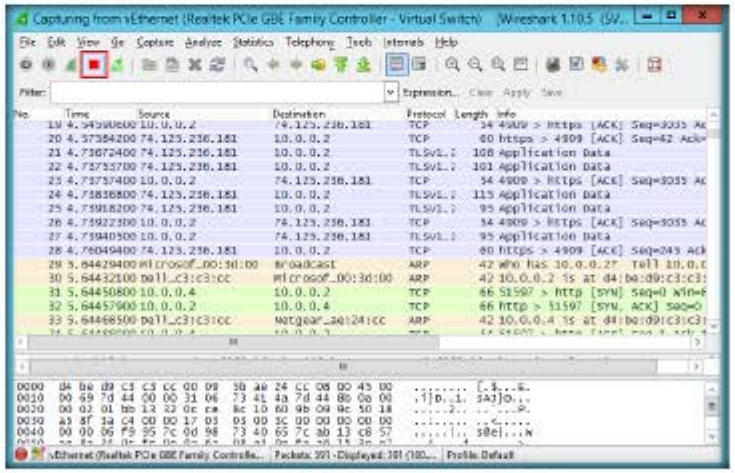


FIGURE 2.25: Stopping the Packet Capture in Wireshark

36. Stop ARP poisoning in Cain & Abel by clicking **Start/Stop APR** in the toolbar.

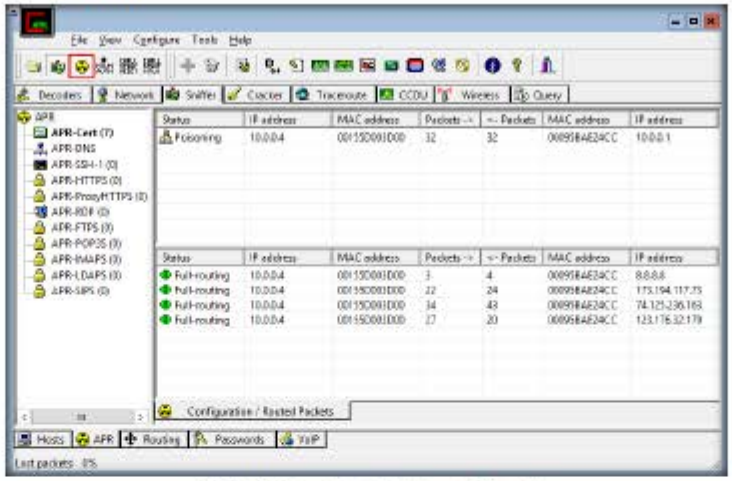


FIGURE 2.26: Stopping the Packet Capture in Wireshark

37. Switch to the Wireshark window. Here, you need to trace the packet containing the current user session's (GoodShopping) cookie.

38. Because there are many packets captured by Wireshark, we shall be using filters to narrow the cookie search.

39. Issue the query **ip.addr==10.0.0.4&&http.cookie** in the **Filter** field, and click **Apply**.

Note: The **10.0.0.4** in the query corresponds to the IP address of **Windows 8.1** virtual machine, which might differ in your lab environment.

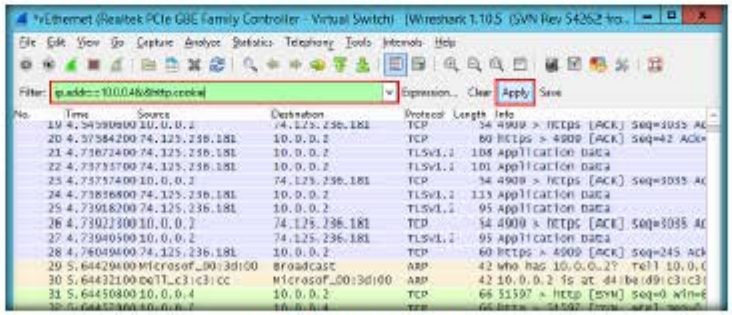


FIGURE 2.27: Filtering the cookie

TASK 5

Filter the packets containing Cookies

40. By issuing the query, Wireshark filters the packets and displays only those packets containing the IP address **10.0.0.4** and a **cookie,** as shown in the screenshot:

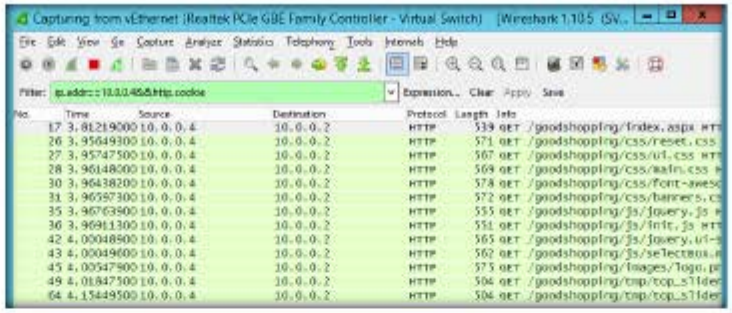


FIGURE 2.28: Wireshark displaying the filtered cookies

41. Now, you need to search for the packet containing the session cookie. Search for the packet containing the URL **goodshopping/index.aspx** (under **Packet list**).

42. You are using this cookie to access http://10.0.0.2/goodshopping/index.aspx directly, without entering user credentials.

Note: Normally, without assigning the cookie value, if you enter http://10.0.0.2/goodshopping/index.aspx, you will be redirected to http://10.0.0.2/goodshopping/login.aspx.

43. Under **Packet details**, expand the **Hypertext Transfer Protocol** node, and click **cookie**.

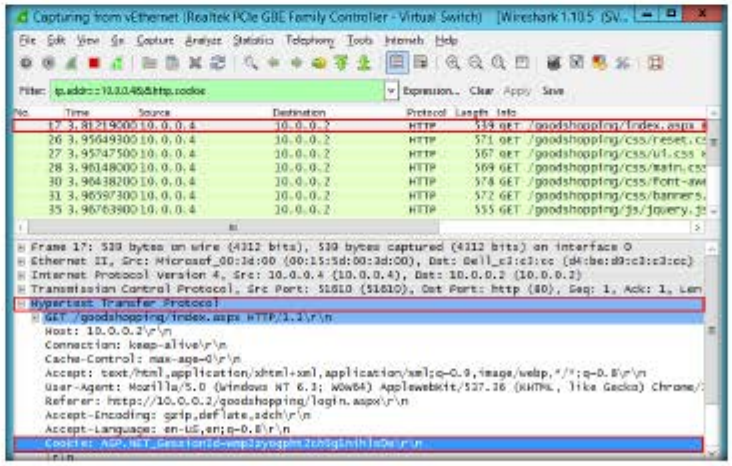


FIGURE 2.29: Selecting the Cookie

44. Right-click the cookie, and select **Copy → Bytes → Printable Text Only**.

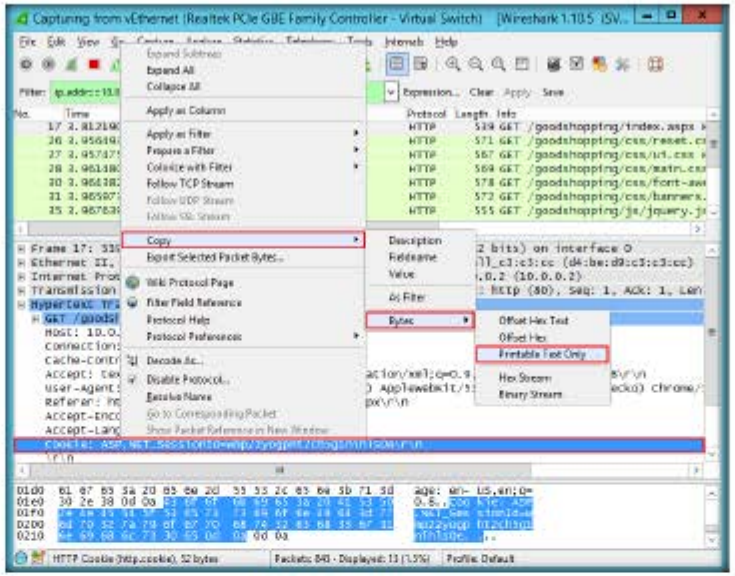


FIGURE 2.30: Copying the Cookie

45. Open a new Notepad window, click **Edit** in the menu bar, and choose **Paste**.

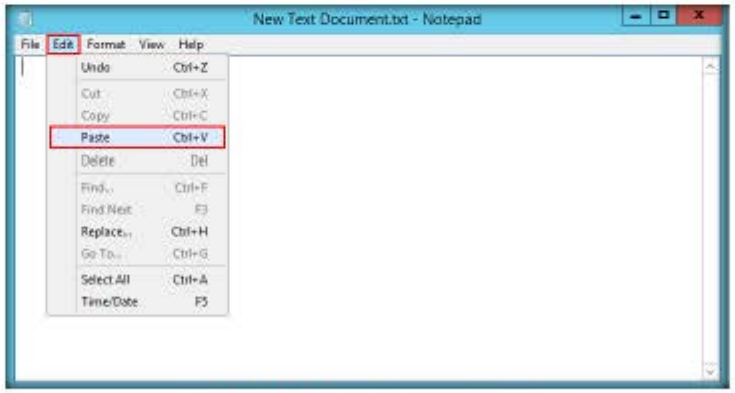


FIGURE 2.31: Pasting the cookie content into notepad

46. The copied cookie will be pasted into Notepad, as shown in the screenshot:

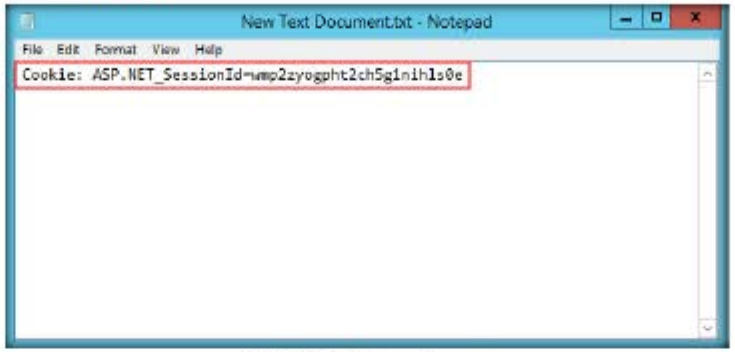


FIGURE 2.32: Cookie pasted in notepad

TASK 6

Install Firebug

47. Now, launch the Firefox web browser, type https://addons.mozilla.org/en-US/firefox/addon/firebug in the address bar, and press **Enter**.

Note: If you have already installed Firebug, skip to **Step 55**.

48. The Firebug add-on webpage appears; click **Add to Firefox**.

FIGURE 2.33: Downloading Firebug add-on to Firefox

49. The add-on begins to download.

50. On completion of the download, a **Software Installation** dialog-box appears; click **Install Now**.

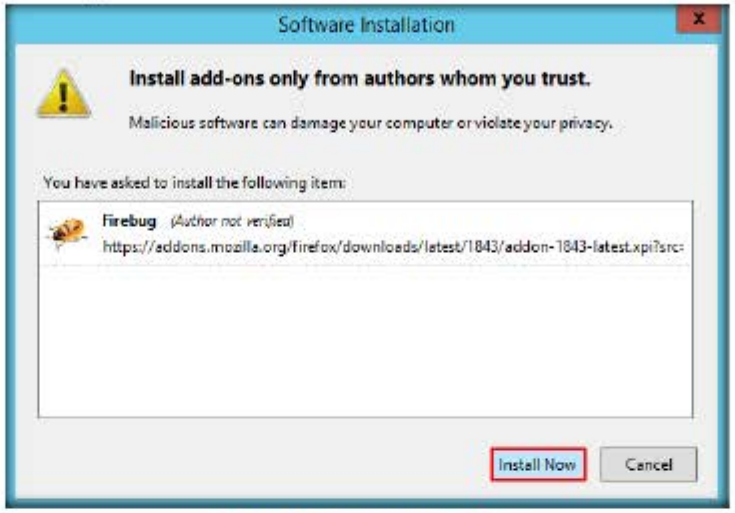


FIGURE 2.34: Software Installation dialog-box

51. On successful installation, the Firebug add-on appears on the top-right corner of the **Navigation Toolbar**, as shown in the screenshot:

FIGURE 2.35: Firebug add-on installed to Firefox

TASK 7

Perform Session Hijacking

52. Now, close the web browser, then re-launch it. Type the URL http://10.0.0.2/goodshopping in the address bar, and press **Enter**.
53. Click **Firebug** on the **Navigation Toolbar**.

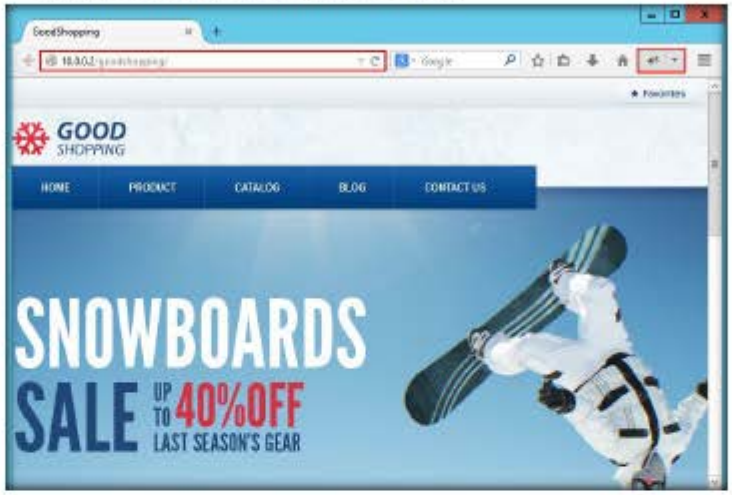


FIGURE 2.36: Activating Firebug

54. The Firebug panel appears in the lower part of the window. Click the **Cookies** tab (on the Firebug panel's menu bar), and click **Enable**.

Note: If cookies are already enabled, skip to the next step.

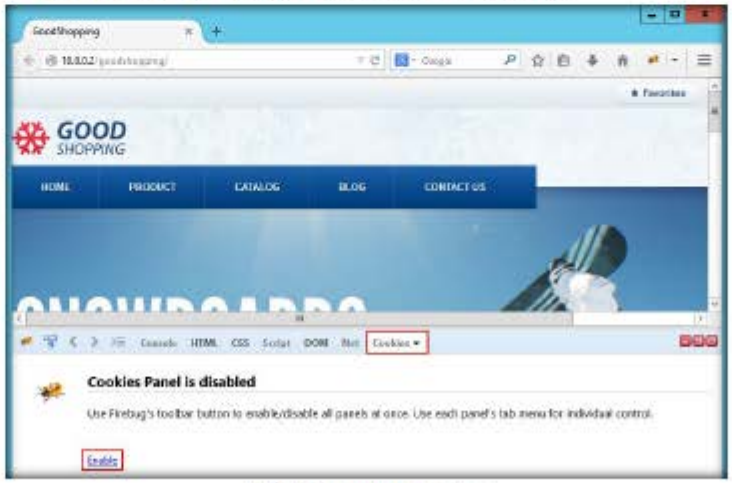


FIGURE 2.37: Enabling Cookies Panel

55. Click the **Cookies** tab, and select **Create Cookie**.

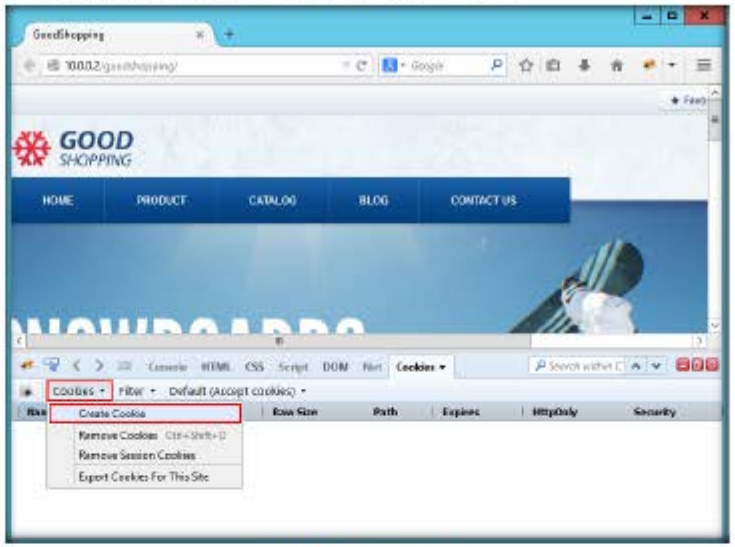


FIGURE 2.38: Creating Cookies

56. The **Edit Cookie** pop-up appears; switch to **Notepad**, copy the cookie name, and paste it in the **Name** field of the **Edit Cookie** pop-up.

57. In the **Host** field, type the IP address of the machine hosting the website. If the IP address is already present, ignore the field.

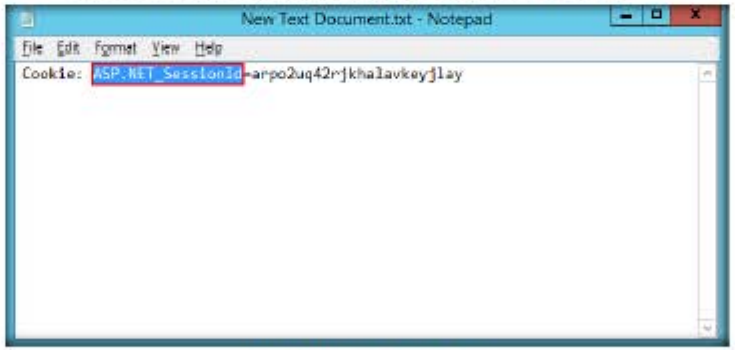


FIGURE 2.39: Copying the Cookie name

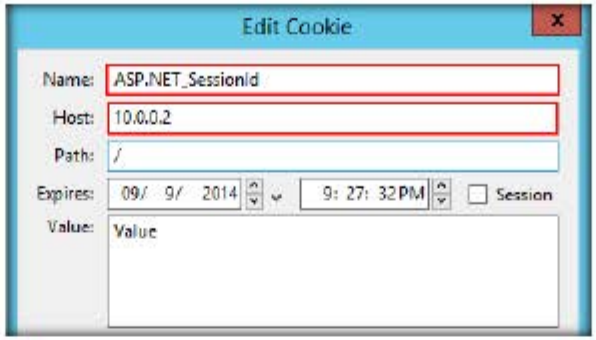


FIGURE 2.40: Adding the cookie Name in Edit Cookie pop-up

58. The cookie name (**ASP.NET_SessionId**) remains constant during the lab, but its value might vary in your lab environment.

59. Copy the cookie value, paste it in the **Value** field, and click **OK**.

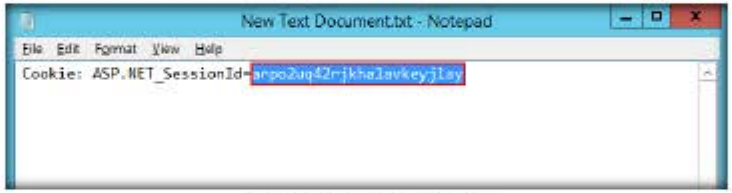


FIGURE 2.41: Copying the Cookie value

FIGURE 2.42: Adding the Cookie value in Edit Cookie pop-up

60. Now, change the URL of the address bar to http://10.0.0.2/goodshopping/index.aspx and press **Enter**.

Note: Normally, without assigning the cookie value, upon entering http://10.0.0.2/goodshopping/index.aspx, you would be redirected to http://10.0.0.2/goodshopping/login.aspx.

61. Observe that you have successfully logged into the website by using the cookies pertaining to the active user session on the **Windows 8.1** machine.

62. Click (at the right edge of the Firebug panel) to deactivate the add-on.

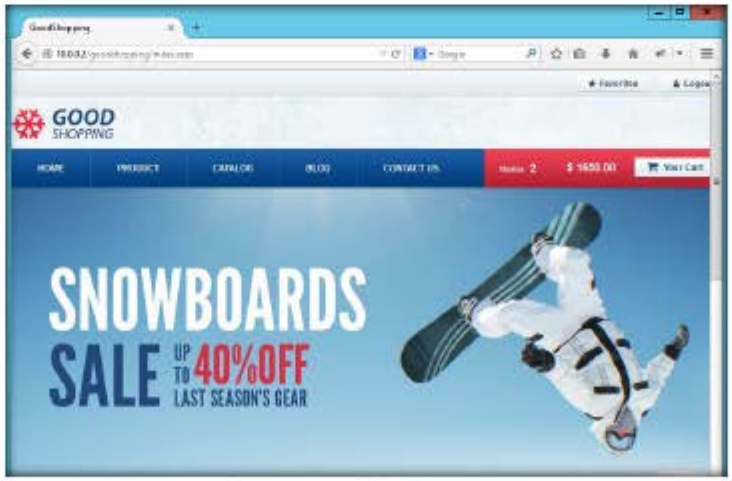


FIGURE 2.43: Successfully gained the user session

63. Now, as you have successfully logged in, you will be able to browse the website and access various web pages as an authenticated user.

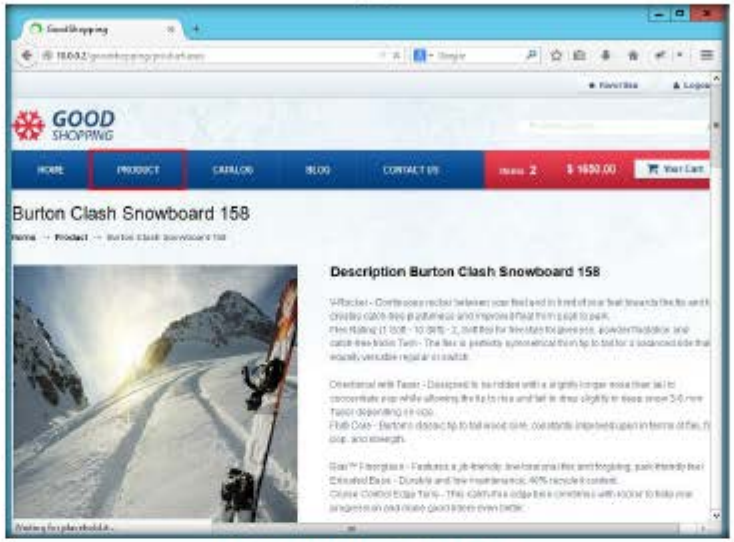


FIGURE 2.44: Clicking the PRODUCT tab

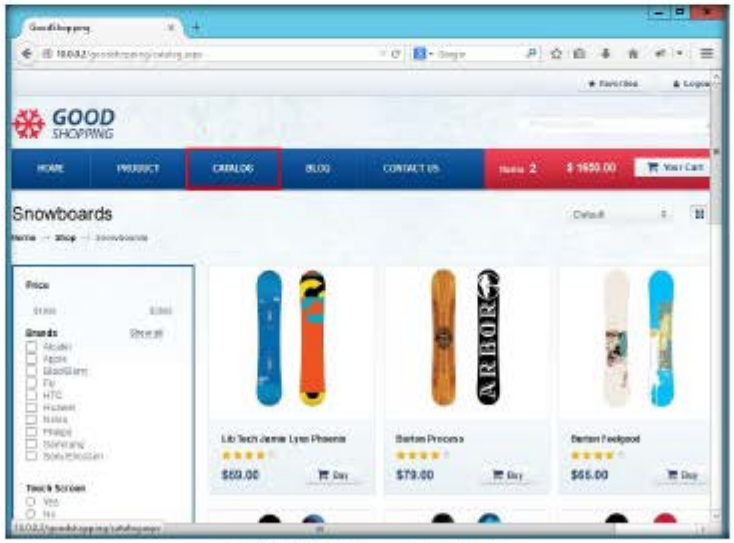


FIGURE 2.45: Clicking the CATALOG tab

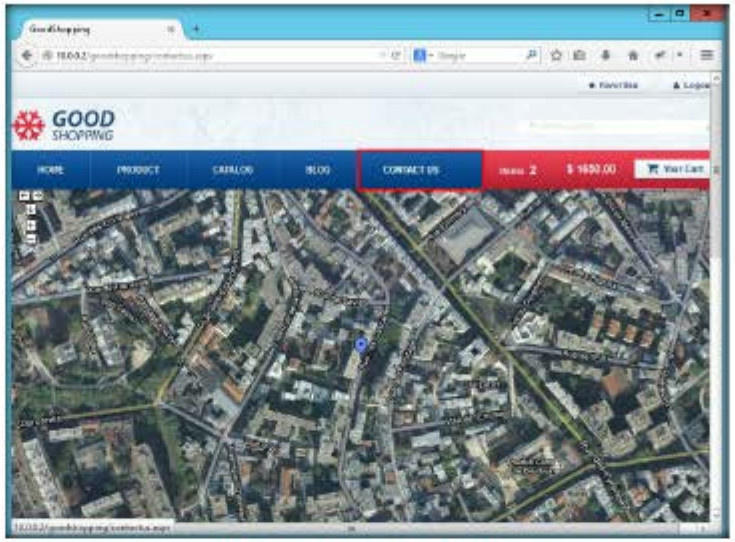


FIGURE 2.46: Clicking the CONTACT US tab

64. Thus, by manipulating the cookies using Firebug, an attacker may simulate session hijacking techniques to gain unauthorized access to an authenticated user session.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

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

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

Lab 3

Hijacking HTTPS Traffic in a Network Using sslstrip

sslstrip is an SSL stripping proxy designed to make unencrypted HTTP sessions mimic HTTPS sessions. It converts https links to http or https using a known private key. It even provides a padlock favicon to simulate a secure channel.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

An attacker usually hijacks a session by exploiting the vulnerabilities in mechanisms used for session establishment. During the development process, developers implement Secure Sockets Layer (SSL) to encrypt all the information in transit via the network. However, attackers can use tools such as sslstrip to sniff clear-text information from HTTPS traffic.

As an ethical hacker or a penetration tester, you most understand the working of SSL-striping tools.

Lab Objectives

The objective of this lab is to learn how to:

- Intercept the Traffic between server and client
- How SSLSTRIP replace HTTPS link with HTTP

Lab Environment

In this lab, you will need:

- A computer running Windows Server 2012 as host machine
- Kali Linux on virtual machine as Attacker Machine
- Windows 8.1 running on virtual machine as target machine
- Administrative privileges to run tools
- A web browser with internet access

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 10 Session Hijacking

Note: This lab will work on Internet Explorer. In this lab, we used 11.0.9 version.

Lab Duration

Time: 15 Minutes

Overview of Lab

This lab will demonstrate HTTPS stripping attacks. sslstrip transparently hijack HTTP traffic with in a network, watch for HTTPS links and redirects, and then map those links into either lookalike HTTP links or homographically-similar HTTPS links.

Lab Tasks

TASK 1

Find Live Hosts

1. Before starting this lab, we need to find live **Hosts** within the network. To find the live hosts, we have tools such as **nmap**.
2. Launch a command terminal in Kali Linux, type **nmap -sP <Network Address Range>**, and press **Enter**. This command will scan the range and list the live hosts in the network, as shown in the figure.
3. Here, we are providing the network range **10.0.0.1/15,** which may vary in your lab environment.
4. We are choosing the target IP address of the **Windows 8.1** machine: **10.0.0.9.**

   Note: The IP addresses shown in this lab may vary in your lab environment.

This command will discover the Live Hosts with in the Network.

```
root@kali:~# nmap -sP 10.0.0.1/15

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-16 08:10 EDT
Nmap scan report for 10.0.0.1
Host is up (0.0013s latency).
MAC Address: 4C:60:DE:CD:FF:02 (Netgear)
Nmap scan report for 10.0.0.2
Host is up (0.0013s latency).
MAC Address: D4:BE:D9:C3:C3:CC (Dell)
Nmap scan report for 10.0.0.4
Host is up (0.0013s latency).
MAC Address: 00:15:5D:3C:EE:02 (Microsoft)
Nmap scan report for www.moviescope.com (10.0.0.5)
Host is up (0.00037s latency).
MAC Address: A4:1F:72:81:F2:D5 (Dell)
Nmap scan report for 10.0.0.7
Host is up (0.0012s latency).
MAC Address: 00:15:5D:3C:EE:01 (Microsoft)
Nmap scan report for 10.0.0.9
Host is up (0.00072s latency).
MAC Address: 00:15:5D:00:27:00 (Microsoft)
Nmap scan report for 10.0.0.6
Host is up.
```

FIGURE 3.1: Finding Live Hosts in a Network

5. By default, in any Linux machine, IP forwarding is disabled. So you first need to enable IP forwarding in your Kali Linux machine.
6. Now, type **echo 1 > /proc/sys/net/ipv4/ip_forward** and press **Enter**. This command enables IP forwarding in your Kali Linux machine. These settings are not preserved after a reboot.

To check the status of IP forwarding at any time, issue the following command: cat /proc/sys/net/ipv4/ip_forward
If the above command returns a 1, IP forwarding is enabled. If it returns a 0, then you must issue the echo command listed above.

FIGURE 3.2: IP Forwarding in Kali Linux

7. We need to set up a firewall rule, using **iptables** to redirect the requests from port **80** to port **8080**, which will ensure that outgoing traffic from the SSL strip is routed from the correct port.
8. Now, type **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080** and press **Enter**.
9. Once you have finished the IP table configuration, **minimize** the command terminal.

FIGURE 3.3: Configuring IPtables

TASK 2

Performing ARPSPOOFING

10. We need to redirect all the network HTTP traffic by using **ARPSPOOF**.
11. To employ arpspoofing, open a new command terminal window, and type **arpspoof -i eth0 -t <Target Machine IP address> <Default Gateway>**; then press **Enter**.
12. Here, we are providing IP address of the **Windows 8.1** machine and the **Default Gateway** of the network (i.e., **10.0.0.1**). The IP address and Default gateway may differ in your lab environment.
13. Once run, arpspoof starts capturing network traffic. You can see the relay of traffic in the command terminal.

FIGURE 3.4: Performing ARPSPOOFING on Target Machine

TASK 3

Starting sslstrip

14. Now, we will strip the SSL layer off from our victim machine.
15. After running arpspoof, maximize the window in which you have configured IP tables; or open a new command terminal, type **sslstrip -p -l 8080** and press **Enter**.
16. This command will attempt to replace a secure encrypted webpage with their plain-text format, and monitor the data being sent out on port 8080.

"-l" tells the system to listen on specified port.

17. Sslstrip starts running, and then waits for the victim to navigate to a website.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@kali:~# sslstrip -p -l 8080

sslstrip 0.9 by Moxie Marlinspike running...
```

FIGURE 3.5: Running SSLSTRIP

TASK 4

Record SSLSTRIP logs

18. Open a new command terminal window, type **tail -f sslstrip.log** and press **Enter**.
19. This command will record the **SSLSTRIP** logs.

```
root@kali:~# tail -f sslstrip.log
```

FIGURE 3.6: Command to record SSLSTRIP logs

20. Now, switch to the **Windows 8.1** victim machine, and open Internet Explorer.

FIGURE 3.7: Windows 8.1 Victim Machine

21. The victim will open an **HTTPS** page in the browser, but on doing so, the **HTTPS** page will become an **HTTP** one, and the sslstrip will begin capturing traffic.
22. In this lab, type https://www.facebook.com in the address bar, and press **Enter**. SSLSTRIP will change https://www.facebook.com to http://www.facebook.com.

Inside the SSL Strip folder there will be a new file created "sslstrip.log" that stores all information that already captured over the HTTP protocol and even the HTTPS.

FIGURE 3.8: HTTPS page in Internet Explorer

23. SSLSTRIP shows you the actual webpage, as in the figure below.
24. Now, type the **username** and **password** and click **Login**.

FIGURE 3.9: Victim is Logging in SSLSTRIP page

25. Now switch to the Kali Linux machine, and **maximize** the arpspoof window. After capturing enough data, press **CTRL+C** to stop arpspoofing.
26. Maximize the sslstrip.log terminal window, and press **CTRL+C** to stop the traffic, after gathering enough data via sslstrip. View the logs recorded by the sslstrip.log.
27. **SSLSTRIP** has captured the username and password from the victim machine, as shown in the screenshot.

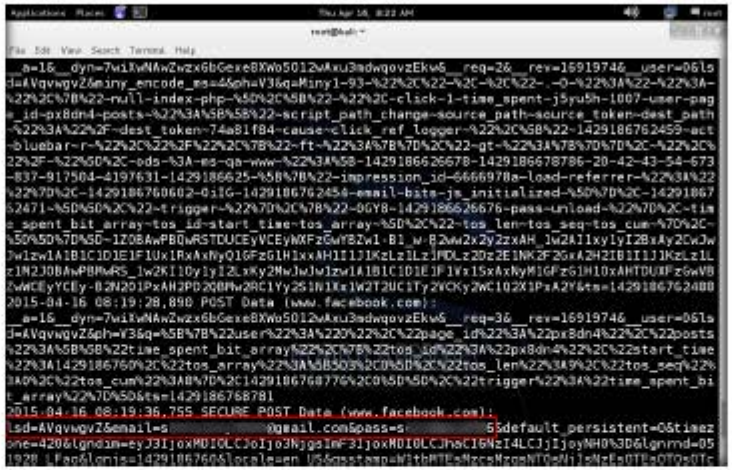


FIGURE 3.10: Captured Username and Password

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 4

Performing a MITM Attack and Hijacking an Established Session Using Websploit

Websploit is an Advanced MITM framework used to scan and exploit target services from the Metasploit framework.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers can use session hijacking to launch various kinds of attacks, such as man-in-themiddle (MITM) and DoS attacks. An MITM attack is one in which the attacker places himself between the client and server. Session hijacking enables 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 an ethical hacker or a penetration tester, you must know the working of a 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 between server and client

Lab Environment

In this lab, you will need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 10 Session Hijacking

- A computer running Windows Server 2012 as Host machine
- A computer running Kali Linux on virtual machine as Attacker Machine
- A computer running Windows 8.1 running on virtual machine as Target machine
- 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 the victim's machine by using a proxy and also how to view all the requests and responses that attacker receives from the victim's machine.

Lab Tasks

TASK 1

Launch Websploit Framework

1. Before starting this lab, ensure that the Windows 8.1 machine (Victim) is turned on.
2. Launch the Kali Linux machine (Attacker), and open a command terminal. Type **websploit** and press **Enter**.
3. The **websploit** shell appears, as shown in the figure below.

FIGURE 4.1: Launch Websploit

4. Search for attack modules in **websploit** by typing **show modules** in the **wsf** shell and pressing **Enter**.
5. This command will list out all the available modules in the websploit.
6. Now, choose the method of exploit to run in the victim machine.

7. In this lab, we are going to perform a man-in-the-middle (**MITM**) attack on the network.

```
msf > show modules

Web Modules                    Description
-----------                    -----------
web/apache_users               Scan Directory Of Apache Users
web/dir_scanner                Directory Scanner
web/wmap                       Information Gathering From Victim Web Using (Metasploit
 Wmap)
web/pma                        PHPMyAdmin Login Page Scanner
web/cloudflare_resolver        CloudFlare Resolver

Network Modules                Description
---------------                -----------
network/arp_dos                ARP Cache Denial Of Service Attack
network/mfod                   Middle Finger Of Doom Attack
network/mitm                   Man In The Middle Attack
network/mlitm                  Man Left In The Middle Attack
network/webkiller              TCP Kill Attack
network/fakeupdate             Fake Update Attack Using DNS Spoof
network/arp_poisoner           Arp Poisoner
```

FIGURE 4.2: Webspoit Modules

TASK 2

Use Type of Exploit

8. Type **use network/mitm** and press **Enter** to display a new MITM shell within the websploit framework shell.

```
Network Modules                Description
---------------                -----------
network/arp_dos                ARP Cache Denial Of Service Attack
network/mfod                   Middle Finger Of Doom Attack
network/mitm                   Man In The Middle Attack
network/mlitm                  Man Left In The Middle Attack
network/webkiller              TCP Kill Attack
network/fakeupdate             Fake Update Attack Using DNS Spoof
network/arp_poisoner           Arp Poisoner

Exploit Modules                Description
---------------                -----------
exploit/autopwn                Metasploit Autopwn Service
exploit/browser_autopwn        Metasploit Browser Autopwn Service
exploit/java_applet            Java Applet Attack (Using HTML)

Wireless / Bluetooth Modules   Description
----------------------------   -----------
wifi/wifi_jammer               Wifi Jammer
wifi/wifi_dos                  Wifi Dos Attack
wifi/wifi_honeypot             Wireless Honeypot(Fake AP)
bluetooth/bluetooth_pod        Bluetooth Ping Of Death Attack

msf > use network/mitm
msf:MITM >
```

FIGURE 4.3: Using Exploit

9. Before the exploit, we need to set the options. Type **show options** and press **Enter**.

10. This command will list the options in the network for specifying the network router and target machine IP addresses. You can also specify the SNIFFER to sniff the victim machine.

11. In this lab, we are going to specify **ROUTER** and **TARGET** machine IP addresses and we will leave all other default settings.

```
wifi/wifi_jammer                Wifi Jammer
wifi/wifi_dos                   Wifi Dos Attack
wifi/wifi_honeypot              Wireless Honeypot(Fake AP)
bluetooth/bluetooth_pod         Bluetooth Ping Of Death Attack

msf > use network/mitm
msf:MITM > show options

Options          Value                          RQ      Description
--------         -------------                  ----    -------------
Interface        eth0                           yes     Network Interface Name
ROUTER           192.168.1.1                    yes     Router IP Address
TARGET           192.168.1.2                    yes     Target IP Address
SNIFFER          driftnet                       yes     Sniffer Name (Select From Sniff
er List)
SSL              true                           yes     SSLStrip, For SSL Hijacking(tru
e or false)

Sniffers         Description
-----------      -------------
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM >
```

FIGURE 4.4: View Options

TASK 3

Set Target Network

12. To set the router, type **set ROUTER <Gateway IP Address>** and press **Enter**.
13. In this lab, we are on the **10.0.0.1** network, which might differ in your lab environment.

```
wifi/wifi_dos                   Wifi Dos Attack
wifi/wifi_honeypot              Wireless Honeypot(Fake AP)
bluetooth/bluetooth_pod         Bluetooth Ping Of Death Attack

msf > use network/mitm
msf:MITM > show options

Options          Value                          RQ      Description
--------         -------------                  ----    -------------
Interface        eth0                           yes     Network Interface Name
ROUTER           192.168.1.1                    yes     Router IP Address
TARGET           192.168.1.2                    yes     Target IP Address
SNIFFER          driftnet                       yes     Sniffer Name (Select From Sniff
er List)
SSL              true                           yes     SSLStrip, For SSL Hijacking(tru
e or false)

Sniffers         Description
-----------      -------------
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM > set ROUTER 10.0.0.1
ROUTER => 10.0.0.1
msf:MITM >
```

FIGURE 4.5: Set Router Target

TASK 4

Set Target Machine

14. Set the target machine for which you want to sniff (the Windows 8.1 machine is the victim).
15. To set the target, type **set TARGET <Victim machine IP address>** and press **Enter**.

```
bluetooth/bluetooth_pod        Bluetooth Ping Of Death Attack

msf > use network/mitm
msf:MITM > show options

Options          Value                          RQ      Description
--------         -------------                  ----    -------------
Interface        eth0                           yes     Network Interface Name
ROUTER           192.168.1.1                    yes     Router IP Address
TARGET           192.168.1.2                    yes     Target IP Address
SNIFFER          driftnet                       yes     Sniffer Name (Select From Sniff
er List)
SSL              true                           yes     SSLStrip, For SSL Hijacking(tru
e or false)

Sniffers         Description
-----------      -------------
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM > set ROUTER 10.0.0.1
ROUTER => 10.0.0.1
msf:MITM > set TARGET 10.0.0.3
TARGET => 10.0.0.3
```

FIGURE 4.6: Set Target Machine IP address

16. To verify the settings, type **show options** and press **Enter** (otherwise, skip to the next step).

```
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM > set ROUTER 10.0.0.1
ROUTER => 10.0.0.1
msf:MITM > set TARGET 10.0.0.3
TARGET => 10.0.0.3
msf:MITM > show options

Options          Value                          RQ      Description
--------         -------------                  ----    -------------
Interface        eth0                           yes     Network Interface Name
ROUTER           10.0.0.1                       yes     Router IP Address
TARGET           10.0.0.3                       yes     Target IP Address
SNIFFER          driftnet                       yes     Sniffer Name (Select From Sniff
er List)
SSL              true                           yes     SSLStrip, For SSL Hijacking(tru
e or false)

Sniffers         Description
-----------      -------------
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM >
```

FIGURE 4.7: View Options

17. To exploit the victim machine, type **run** and press **Enter**.

TASK 5

Run Exploit

```
msf:MITM > set ROUTER 10.0.0.1
ROUTER => 10.0.0.1
msf:MITM > set TARGET 10.0.0.3
TARGET => 10.0.0.3
msf:MITM > show options

Options          Value                          RQ      Description
.........        .............                  ....    .............
Interface        eth0                           yes     Network Interface Name
ROUTER           10.0.0.1                       yes     Router IP Address
TARGET           10.0.0.3                       yes     Target IP Address
SNIFFER          driftnet                       yes     Sniffer Name (Select From Sniff
er List)
SSL              true                           yes     SSLStrip, For SSL Hijacking(tru
e or false)

Sniffers         Description
.........        .............
dsniff           Sniff All Passwords
msgsnarf         Sniff All Text Of Victim Messengers
urlsnarf         Sniff Victim Links
driftnet         Sniff Victim Images

msf:MITM > run
[*]IP Forwarding ...
[*]ARP Spoofing ...
[*]Sniffer Starting ...
```

FIGURE 4.8: Running the Exploit

18. A small **driftnet** sniffer window will open, as shown in the figure below. **Maximize** the driftnet window to view the sniffed results.

FIGURE 4.9: Driftnet pop-up

19. Switch to the victim's machine and open a web browser (here, Chrome).
20. In the address bar, type any URL and press **Enter**.

21. In this lab, we are browsing www.cnet.com/news.

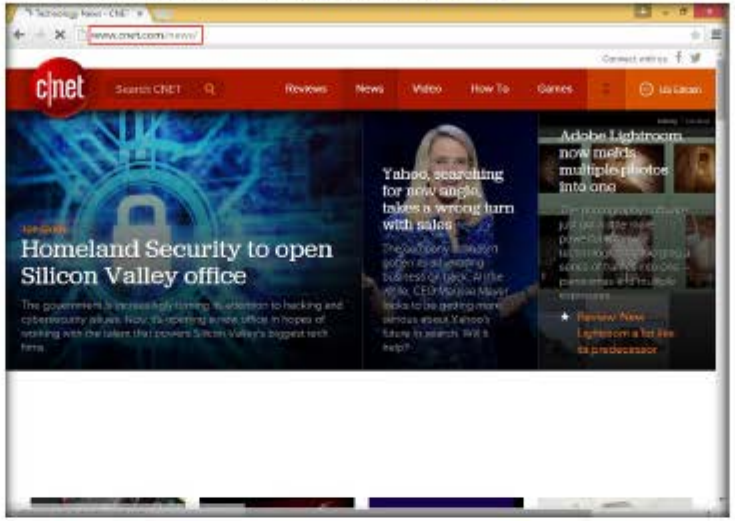


FIGURE 4.10: Victim Machine Browser page

TASK 6

Driftnet Captured Images of Website

22. Switch back to the **Kali Linux** (attacker) machine, and observe the driftnet window. It shows you the browsed website images by the victim.

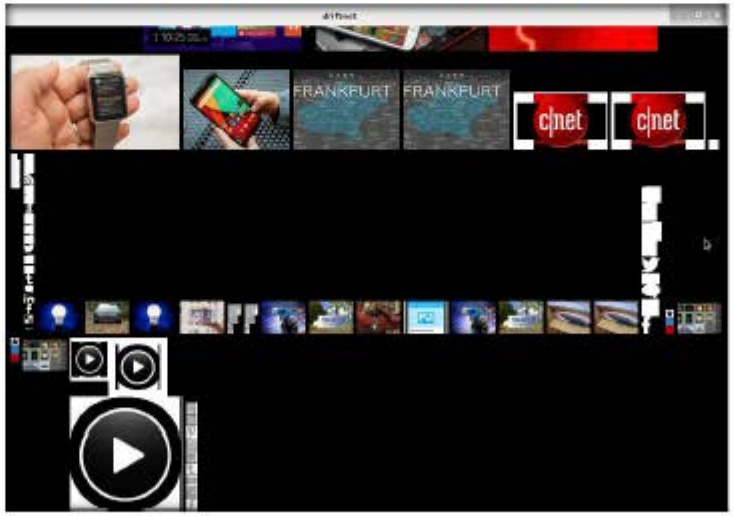


FIGURE 4.11: Driftnet Sniffer Captured Images

23. Driftnet will save the website images in the following location of the attacker machine.

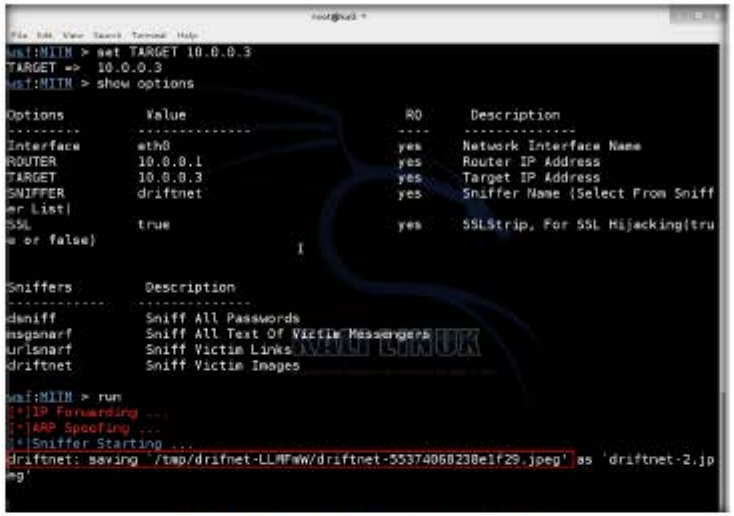


FIGURE 4.12: Driftnet stored Downloaded Images location

24. To view the downloaded images, navigate to the **Places** → **Computer** → **File System** → **tmp** folder, and open the driftnet folder (which can vary with each session).

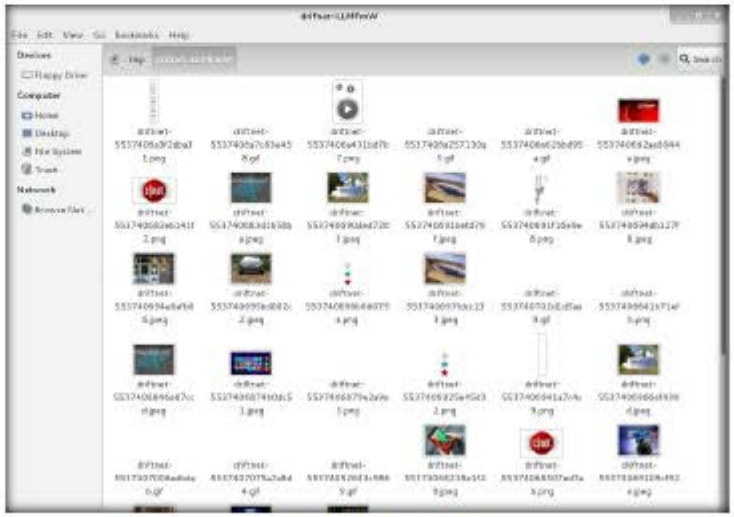


FIGURE 4.13: Driftnet Captured Images

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