Authentication Based Attacks (Contd)

Tools in Kali Linux

Module #28

Kali Linux: Firefox plugins?

The manual method to perform a session hijack is stealing a victim's authentication cookie.

One way to accomplish this is injecting a script on a compromised web application server so cookies are captured without the victim's knowledge. From there, the attacker can harvest authentication cookies and use a cookie injector tool to replace the attacker's cookie with an authorized stolen cookie. Other methods used to steal cookies are packet sniffing, network traffic, and compromising hosts.

The Firefox web browser offers many plugins that can be used to inject stolen cookies into an attacker's browser. Examples are GreaseMonkey, Cookie Manager, and FireSheep.

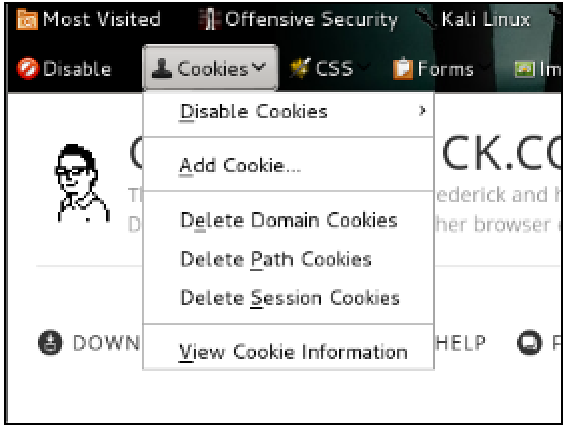
Kali Linux: Web Developer - Firefox plugin?

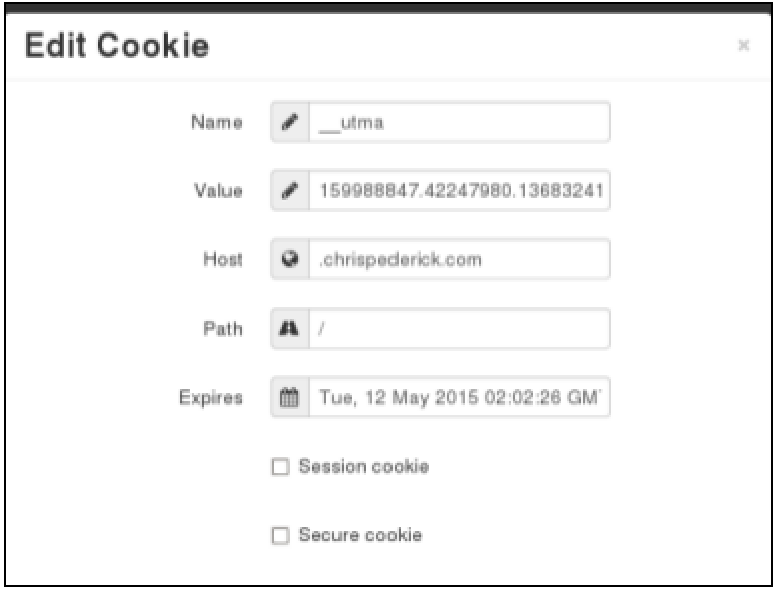
Web Developer is an extension for Firefox that adds editing and debugging tools for web developers. Web Developer can be downloaded for free from the Firefox plugin store. One feature in Web Developer useful for session hijacking is the ability to edit cookies.

This can be found as a drop-down option from the Firefox browser once Web Developer is installed

Kali Linux: Firefox plugin?

Select View Cookie Information, and you will see stored cookies. You can click on Edit Cookie to bring up the cookie editor and replace the current cookie with a victim's stolen cookie.





Edit Cookie

Name __utma

Value 159988847.42247980.13683241

Host .chrispederick.com

Path /

Expires Tue, 12 May 2015 02:02:26 GM

☐ Session cookie

☐ Secure cookie

Kali Linux: Greasemonkey plugin?

Greasemonkey is a Firefox plugin that allows users to install scripts that make on the fly changes to web page content before or after the page is loaded.

Greasemonkey can be used for customizing a web page appearance, web functions, debugging, combining data from other pages, as well as other purposes.

Greasemonkey is required to make other tools, such as Cookie Injector, function properly.

Kali Linux: Cookie Injector plugin?

Cookie Injector is a user script that simplifies the process of manipulating browser cookies.

There are a lot of manual steps to import a cookie from a tool like Wireshark into a web browser.

Cookie Injector allows the user to copy paste a cookie portion of a dump, and have the cookies from the dump automatically created on the currently viewed web page.

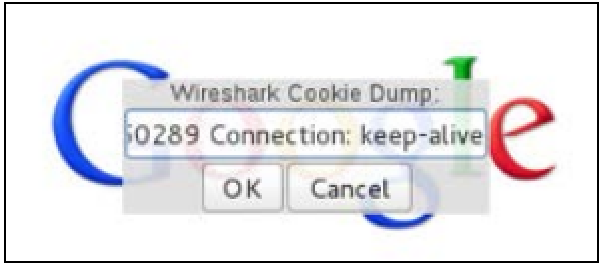
Kali Linux: Cookie Injector plugin?

After installing the Cookie Injector script, press Alt+C to display the cookie dialog. Paste a copied Wireshark string into the input box and click on OK to inject cookies into the current page.

Wireshark tool will be dealt subsequently in this course with examples

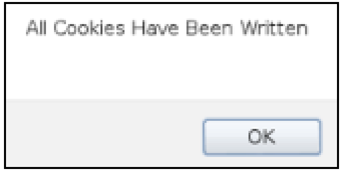
The next two screenshots show pressing Alt+C, pasting a Wireshark Cookie Dump, and clicking OK to see the pop-up that the captured cookies have been written into the Internet browser.

Kali Linux: Cookie Injector plugin?



Wireshark Cookie Dump:

;0289 Connection: keep-alive



All Cookies Have Been Written

Kali Linux: Cookies Manager+ plugin?

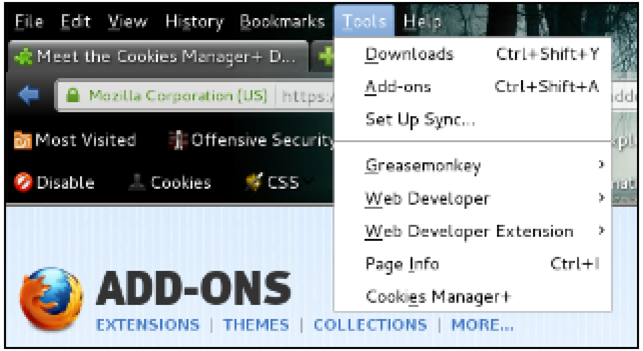
Cookies Manager+ is a utility used to view, edit, and create new cookies. Cookie Manager+ shows detailed information about cookies, as well as can edit multiple cookies at once.

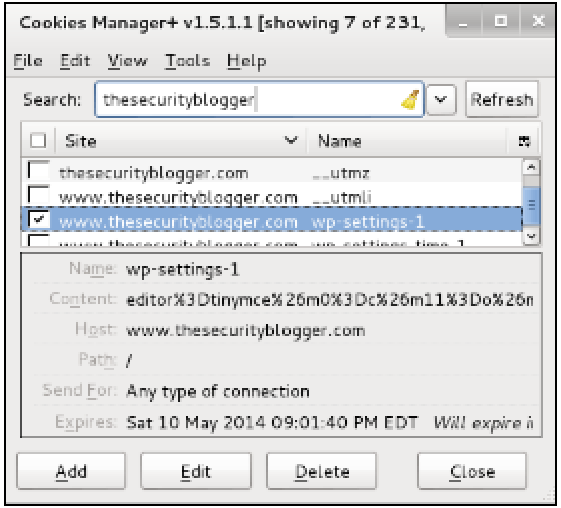
Can also back up and restore cookies. You can download from Firefox plugin store.

Once installed, Cookie Manager+ can be accessed under Tools, by selecting Cookies Manager+.

Cookies Manager+ will show you all cookies captured by Firefox. You can scroll down or search for specific Cookie(s) to view and/or edit.

Kali Linux: Cookies Manager+ plugin?




Cookies Manager+ v1.5.1.1 [showing 7 of 231,
File Edit View Tools Help
Refresh
Add
Edit
Delete
Close

Search: thesecurityblogger

	Site	Name
□	thesecuritybIogger.com	__utmz
□	www.thesecurityblogger.com	__utmli
☑	www.thesecurityblogger.com	wp-settings-1
□	www.thesecurityblogger.com	wp-settings-time-1

Name: wp-settings-1

Content: editor%3Dtinymce%26m0%3Dc%26m11%3Do%26n

Host: www.thesecurityblogger.com

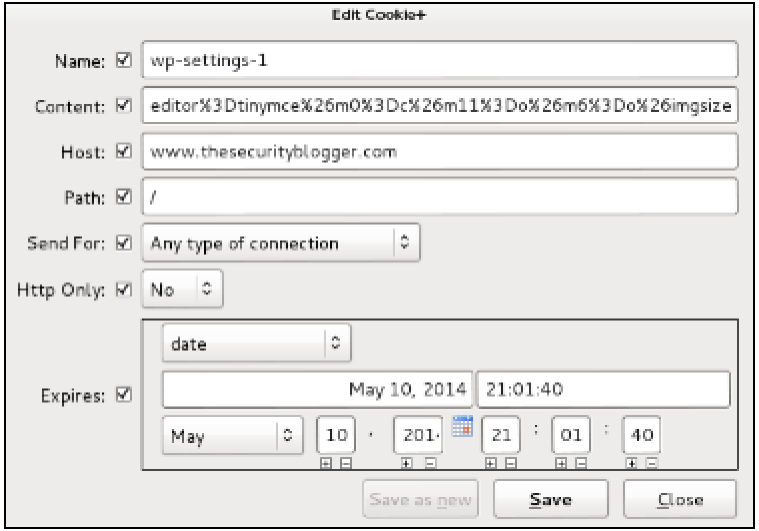
Path: /

Send For: Any type of connection

Expires: Sat 10 May 2014 09:01:40 PM EDT *Will expire i*

Kali Linux: Cookies Manager+ plugin?

Cookies Manager+ makes editing existing cookies easy. This can be useful for performing various types of attacks such as session hijacking and SQL injection.



Name: ☑ wp-settings-1

Content: ☑ editor%3Dtinymce%26m0%3Dc%26m11%3Do%26m6%3Do%26imgsize

Host: ☑ www.thesecurityblogger.com

Path: ☑ /

Send For: ☑ Any type of connection

Http Only: ☑ No

Expires: ☑ date

May 10, 2014 21:01:40

May 10 · 201· 21 : 01 : 40

Kali Linux: Cookie Cadger?

Cookie Cadger is a Penetration Testing tool used to audit web sessions. Cookie Cadger can include detailed HTTP request capturing and replaying insecure HTTP GET requests, such as requested items, user agents, referrer and basic authorization.

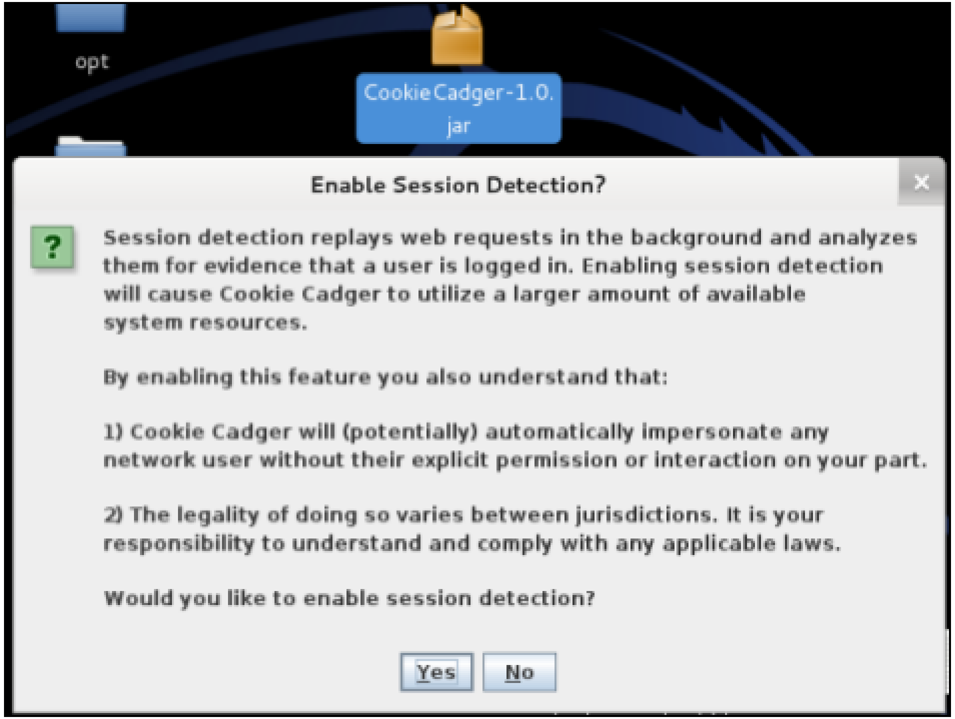
Cookie Cadger can provide live analysis for Wi-Fi and wired networks; as well as load packet capture (PCAP) files. Cookie Cadger also includes session detection to determine if the user is logged into webpages like Wordpress and Facebook.

Kali Linux: Cookie Cadger?

Cookie Cadger can be downloaded from www.cookiecadger.com . The download will be a JAR file.

Double-click on the file to open Cookie Cadger. A warning will pop up asking if you want to enable session detection. Click on Yes, and the main dashboard will pop up.

Kali Linux: Cookie Cadger plugin?



Enable Session Detection?

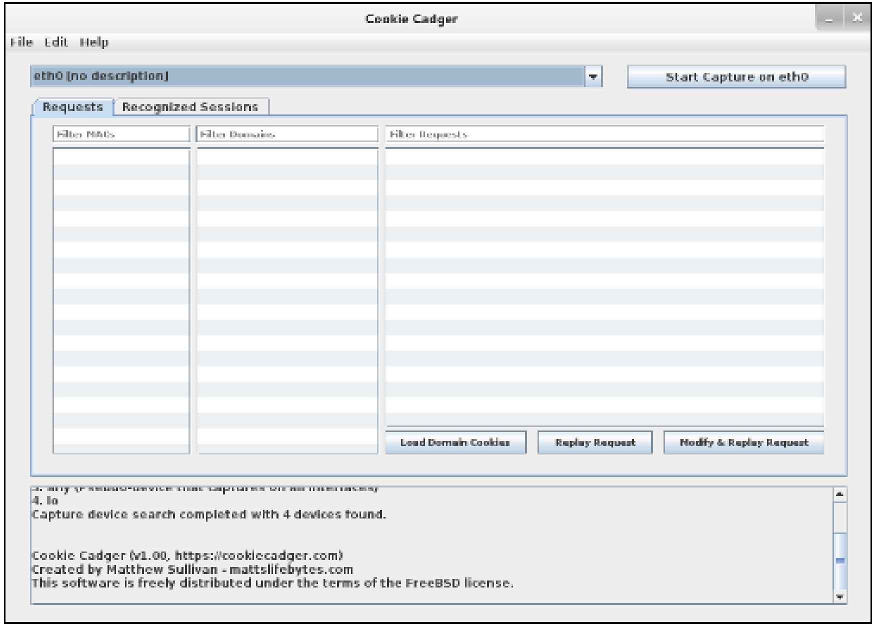
Session detection replays web requests in the background and analyzes them for evidence that a user is logged in. Enabling session detection will cause Cookie Cadger to utilize a larger amount of available system resources.

By enabling this feature you also understand that:

1) Cookie Cadger will (potentially) automatically impersonate any network user without their explicit permission or interaction on your part.

2) The legality of doing so varies between jurisdictions. It is your responsibility to understand and comply with any applicable laws.

Would you like to enable session detection?

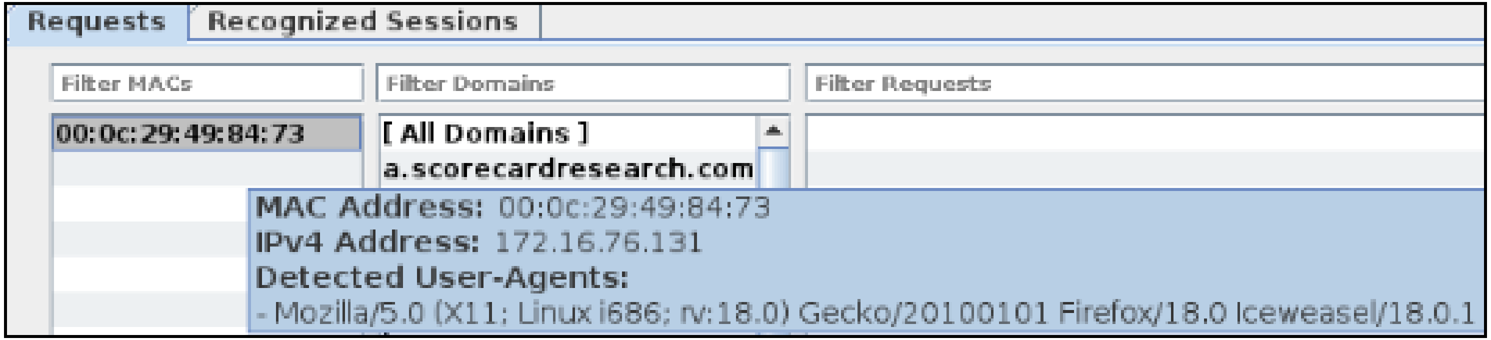


```
3. any (Pseudo-device that captures on all interfaces)
4. lo
Capture device search completed with 4 devices found.


Cookie Cadger (v1.00, https://cookiecadger.com)
Created by Matthew Sullivan - mattslifebytes.com
This software is freely distributed under the terms of the FreeBSD license.
```

Kali Linux: Cookie Cadger plugin?

After you press the 'start capture' key, next screenshot shows a Linux i686 using Firefox and Iceweasel.



MAC Address: 00:0c:29:49:84:73
IPv4 Address: 172.16.76.131
Detected User-Agents:
- Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1

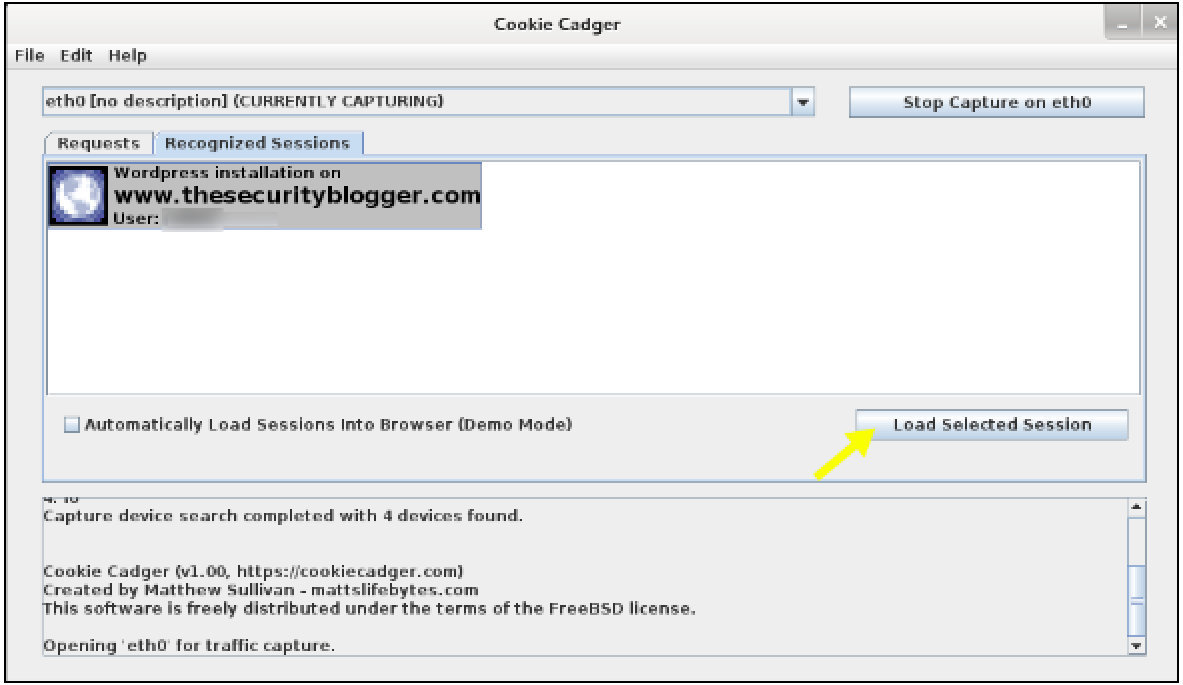
Kali Linux: Cookie Cadger plugin?

When Cookie Cadger recognizes a login session, it captures it and gives the ability to load the session.

The next screenshot shows a session capture of the administrator logging into www.thesecurityblogger.com . Cookie Cadger will show an icon and explain the type of session captured.

This could be a Hotmail, Facebook, or Wordpress login as example

Kali Linux: Cookie Cadger plugin?



eth0 [no description] (CURRENTLY CAPTURING)

Wordpress installation on
www.thesecurityblogger.com
User: [redacted]

□ Automatically Load Sessions Into Browser (Demo Mode)

```
Capture device search completed with 4 devices found.


Cookie Cadger (v1.00, https://cookiecadger.com)
Created by Matthew Sullivan - mattslifebytes.com
This software is freely distributed under the terms of the FreeBSD license.

Opening 'eth0' for traffic capture.
```

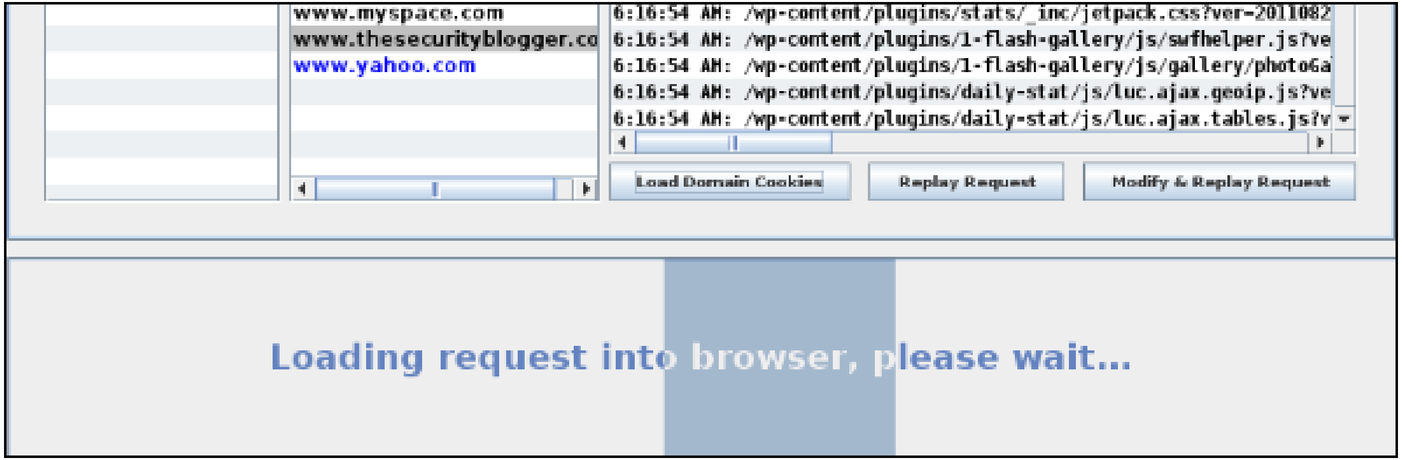
Kali Linux: Cookie Cadger plugin?

To see the recognized sessions, click on the tab labeled Recognized Sessions and pick a session from the window.

Once highlighted, click on the Load Selected Session button to replay the session. Cookie Cadger will display Loading on the bottom window, and a browser will open logged in as the user during the captured session.

Kali Linux: Cookie Cadger plugin?

The screenshot shows opening a Domain cookie captured from the victim. Once the loading is complete, the default Internet browser will open the captured page with the rights associated with the stolen cookie.



www.myspace.com
www.thesecurityblogger.co
www.yahoo.com

```
6:16:54 AM: /wp-content/plugins/stats/_inc/jetpack.css?ver-2011082
6:16:54 AM: /wp-content/plugins/1-flash-gallery/js/swfhelper.js?ve
6:16:54 AM: /wp-content/plugins/1-flash-gallery/js/gallery/photoGa
6:16:54 AM: /wp-content/plugins/daily-stat/js/luc.ajax.geoip.js?ve
6:16:54 AM: /wp-content/plugins/daily-stat/js/luc.ajax.tables.js?v
```

Loading request into browser, please wait...

Thank You