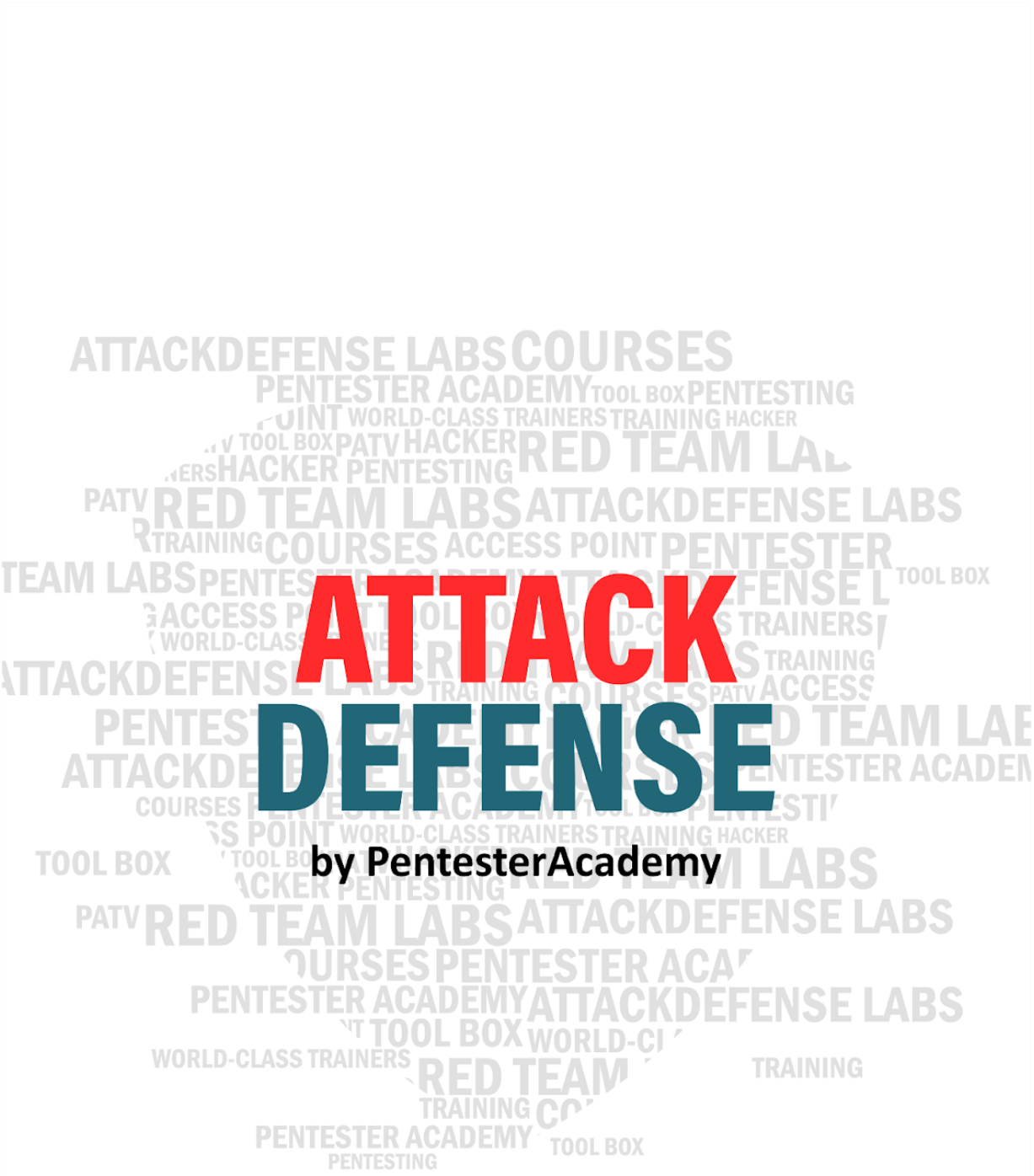
ATTACK
DEFENSE
by PentesterAcademy

Name	T1217: Browser Bookmark Discovery I
URL	https://attackdefense.com/challengedetails?cid=1769
Type	MITRE ATT&CK Linux : Discovery

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Find the URL of the Github repository which is bookmarked in Mozilla Firefox.

Solution:

Step 1: Check the content present in the current working directory.

Commands: ls -l

```
student@attackdefense:~$ ls -l
total 4
drwxr-xr-x 1 student student 4096 Mar 26 02:01 tools
student@attackdefense:~$
```

Step 2: Also list the hidden directories.

Command: ls -al

```
student@attackdefense:~$ ls -al
total 24
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .
drwxr-xr-x 1 root    root    4096 Mar 26 01:59 ..
drwx------ 3 student student 4096 Mar 26 02:01 .cache
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .config
drwxr-xr-x 1 student student 4096 Mar 26 02:01 .mozilla
drwxr-xr-x 1 student student 4096 Mar 26 02:01 tools
student@attackdefense:~$
```

Step 3: Check the contents of tools directory.

Command: ls -l tools/

```
student@attackdefense:~$ ls -l tools/
total 60
drwxr-xr-x 1 student student  4096 Mar 26 01:53 Infornito
-rwxr-xr-x 1 student student 53050 Sep  7  2016 dumpzilla.py
drwxr-xr-x 1 student student  4096 Mar 26 01:53 hindsight
student@attackdefense:~$
```

Step 4: Check the help option for dumpzilla tool.

Command: tools/dumpzilla.py -h

```
student@attackdefense:~$ tools/dumpzilla.py -h

Version: 15/03/2013

Usage: python dumpzilla.py browser_profile_directory [Options]

Options:

 --All (Shows everything but the DOM data. Doesn't extract thumbnails or HTML 5 offline)
 --Cookies [-showdom -domain <string> -name <string> -hostcookie <string> -access <date> -create <
st -range_create <start> <end>]
 --Permissions [-host <string>]
 --Downloads [-range <start> <end>]
 --Forms        [-value <string> -range_forms <start> <end>]
 --History [-url <string> -title <string> -date <date> -range_history <start> <end> -frequency]
 --Bookmarks [-range_bookmarks <start> <end>]
 --Cacheoffline [-range_cacheoff <start> <end> -extract <directory>]
 --Thumbnails [-extract_thumb <directory>]
 --Range <start date> <end date>
 --Addons
 --Passwords (Decode only in Unix)
 --Certoverride
 --Session
 --Watch [-text <string>] (Shows in daemon mode the URLs and text form in real time. -text' Option
xit: Ctrl + C. only Unix).
```

Dumpzilla needs a path to the browser profile directory.

Step 5: Check the path to Firefox browser's profile directory

Command: ls .mozilla/firefox

```
student@attackdefense:~$ ls .mozilla/firefox/
'Crash Reports'   profiles.ini   zevp8nk2.default
student@attackdefense:~$
```

Step 6: List the bookmarks for firefox using dumpzilla tool.

Command: tools/dumpzilla.py .mozilla/firefox/zevp8nk2.default --Bookmarks

```
student@attackdefense:~$ tools/dumpzilla.py .mozilla/firefox/zevp8nk2.default --Bookmarks

[WARNING]: Python 2.x currently used, Python 3.x and UTF-8 is recommended !


================================================================================================
Bookmarks            [SHA256 hash: 29a4f4d8ca1b88f3d9374c7d17e8c2e27ec4d472f45264cf9907239f0670b4ed]
================================================================================================


Title: Help and Tutorials
URL: https://support.mozilla.org/en-US/products/firefox
Date add: 2018-08-01 16:54:58
Last modified: 2018-08-01 16:54:58
```

```
Title: GitHub - ytisf/theZoo: A repository of LIVE malwares for your own joy and pleasure
URL: https://github.com/ytisf/theZoo
Date add: 2018-10-16 23:42:52
Last modified: 2018-10-16 23:42:52
```

The github repo with URL https://github.com/ytisf/theZoo is bookmarked in Firefox.

Flag: https://github.com/ytisf/theZoo

References:

1. Browser Bookmark Discovery (https://attack.mitre.org/techniques/T1217/)
2. Dumpzilla tool (https://github.com/Busindre/dumpzilla)