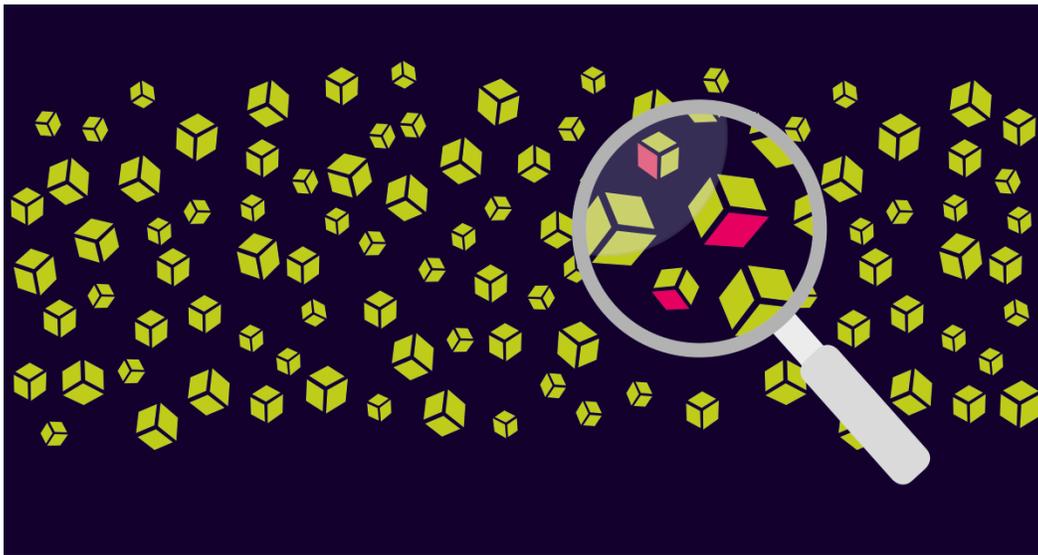




# LAB MANUAL ON A PRACTICAL APPROACH TO NETWORK SNIFFING



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO  
TECHNICAL TEACHERS  
DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
GOVERNMENT OF INDIA

*Principal Investigator: Prof. Maitreyee Dutta*

*Co Investigator: Prof. Shyam Sundar Pattnaik*

**PREPARED BY:**

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

# Table of Contents

---

<b>INTRODUCTION TO NETWORK SNIFFING.....</b>	<b>2</b>
<b>CAIN AND ABEL TOOL.....</b>	<b>3</b>
<b>NETWORK SNIFFING WITH CAIN AND ABEL TOOL.....</b>	<b>4</b>
<b>COUNTERMEASURES.....</b>	<b>22</b>
<b>REFERENCES.....</b>	<b>26</b>

# **MANUAL-2:**

# **A Practical**

# **Approach to**

# **Network**

# **Sniffing**

# INTRODUCTION TO NETWORK SNIFFING

- Network sniffing is a process to sniff the network traffic in real-time.
- It works by capturing and analyzing packets of data that flow through a particular network.
- Figure 1 shows the process of network sniffing where data is travelling through a network in the form of packets. The sniffer intercepts the network traffic and captures the raw data packets.
- The captured data packet is analyzed by the packet sniffing software and presented to the network administrators.

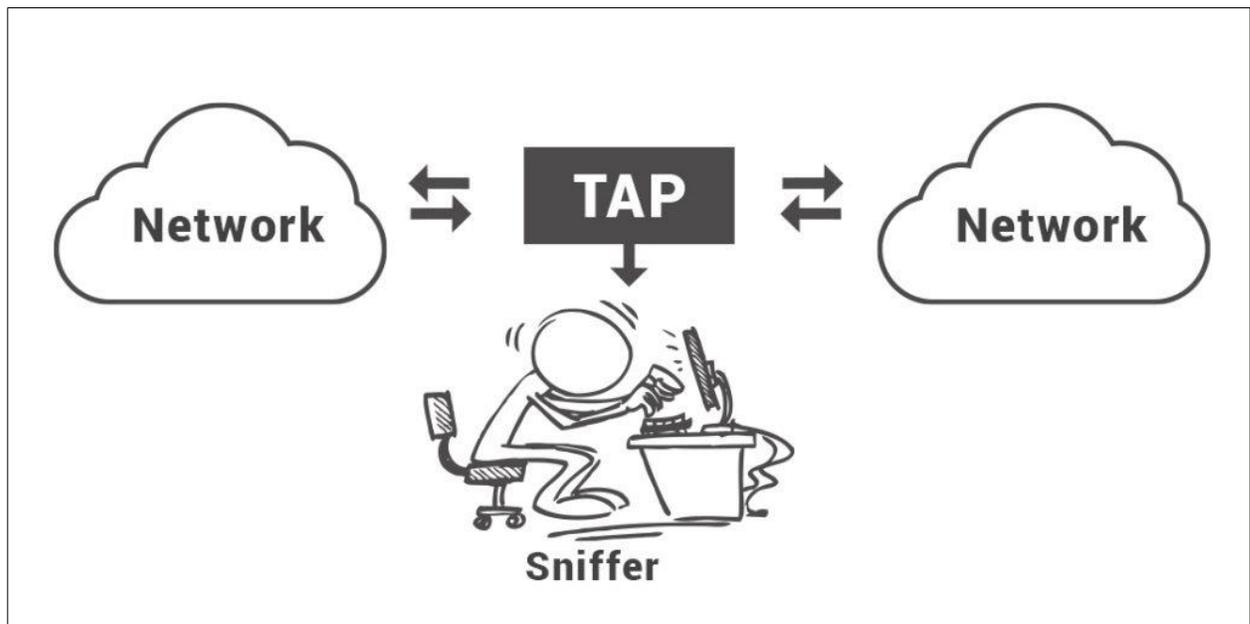


Figure 1: Process of network sniffing

# CAIN AND ABEL TOOL

- The Cain and Abel tool [1] is a password recovery and network sniffing tool which is freely available for Windows operating system.
- This tool is useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons.
- This tool contains features such as Arp Poison Routing (APR) which enables sniffing on switched LANs and wireless network.
- The sniffer can also analyze protocols such as HTTP, SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms.



Figure 2: Cain & Abel tool

# NETWORK SNIFFING WITH CAIN AND ABEL TOOL

Before downloading and installing Cain & Abel tool, it is advised to turn off the Windows firewall and anti-virus tool. The network sniffing can be performed with Cain and Abel tool with following steps:

**Step 1:** Search for Cain & Abel in a searching engine and download the tool as shown in Figure 3 and Figure 4 respectively.

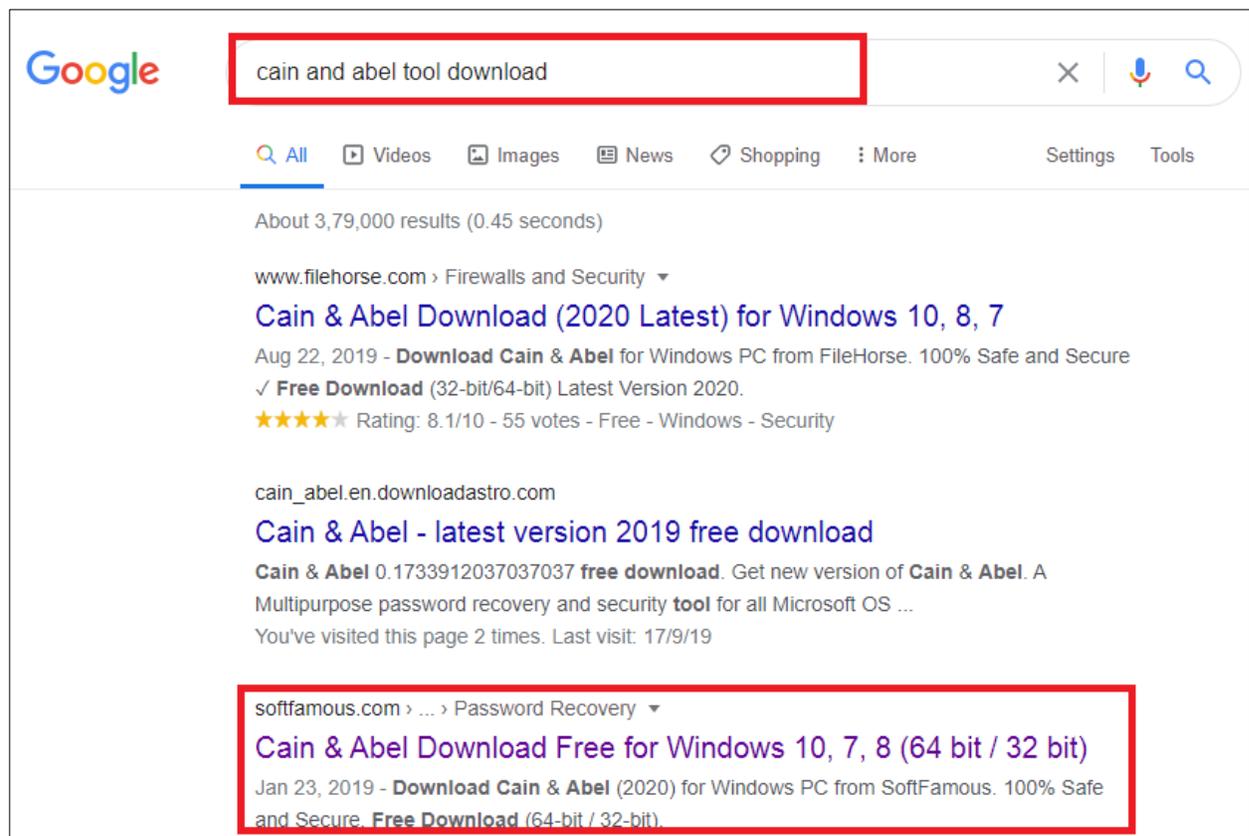


Figure 3: Search Cain and Abel tool

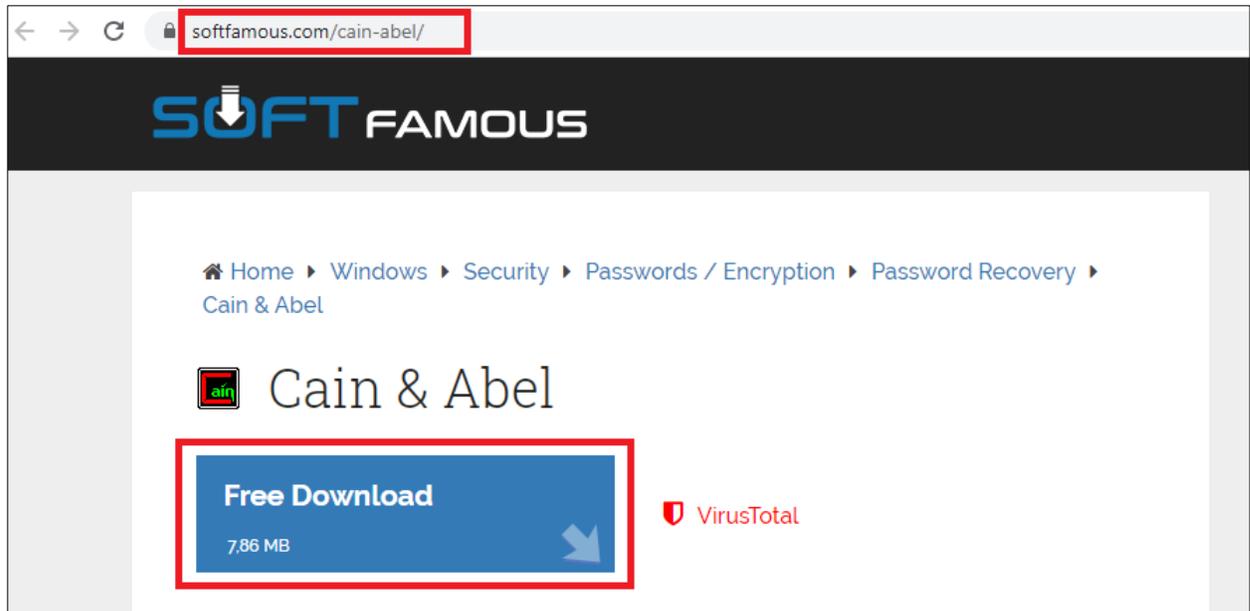


Figure 4: Download Cain and Abel tool

**Step 2:** Download WinPcap for Windows operating system. Figure 5 shows WinPcap for Windows 10 operating system and Figure 6 shows WinPcap for rest of the versions of Windows operating system.

win10pcap.org



# Win10Pcap

New WinPcap-based packet capture library for Windows 10, 8 and 7. Compatible with NDIS 6.x driver model. Supports IEEE802.1Q VLAN tags.

*By Daiyuu Nobori  
University of Tsukuba, Japan*

Overview Download How to use Source code SDK License Japanese

## Win10Pcap: WinPcap for Windows 10 (NDIS 6.x driver model)

Win10Pcap is a new WinPcap-based Ethernet packet capture library.

Unlike original WinPcap, Win10Pcap is compatible with NDIS 6.x driver model to work stably with Windows 10. Win10Pcap also supports capturing IEEE802.1Q VLAN tags.

Win10Pcap has the binary-compatibility with the original WinPcap DLLs. You can run Wireshark or other WinPcap-compatible applications with Win10Pcap by simply installing Win10Pcap DLLs, instead of original WinPcap.

Win10Pcap is written as a personal project by Daiyuu Nobori, a Ph.D student of Computer science of University of Tsukuba, Japan. The many parts of Win10Pcap was from WinPcap.

[Download](#)

- [How to use](#)
- [Source code](#)
- [SDK](#)

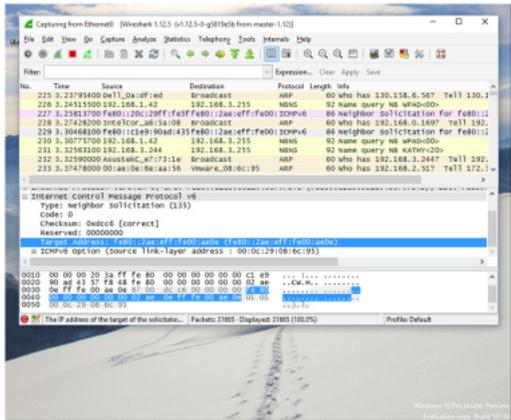


Figure 5: Download WinPcap for Windows 10 operating system

winpcap.org/install/

WiFi Capture Adapter for Windows

**WinPcap Has Ceased Development**  
The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. We recommend using Npcap instead.

If you do insist upon using WinPcap, be aware that its installer was built with an old version of NSIS and as a result is vulnerable to DLL hijacking.

**The last official WinPcap release was 4.1.3**  
For the list of changes, refer to the changelog.

[Version 4.1.3 installer for Windows](#)

Driver +DLLs

**Supported platforms:**

- Windows NT4/2000
- Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)

MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd  
SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cddf448a00

This executable file installs WinPcap on your machine.

Figure 6: Download WinPcap for Windows NT/XP/.../Win8 operating system

**Step 3:** Figure 7 shows icon of Cain & Abel tool on Desktop of Windows operating system after installation.

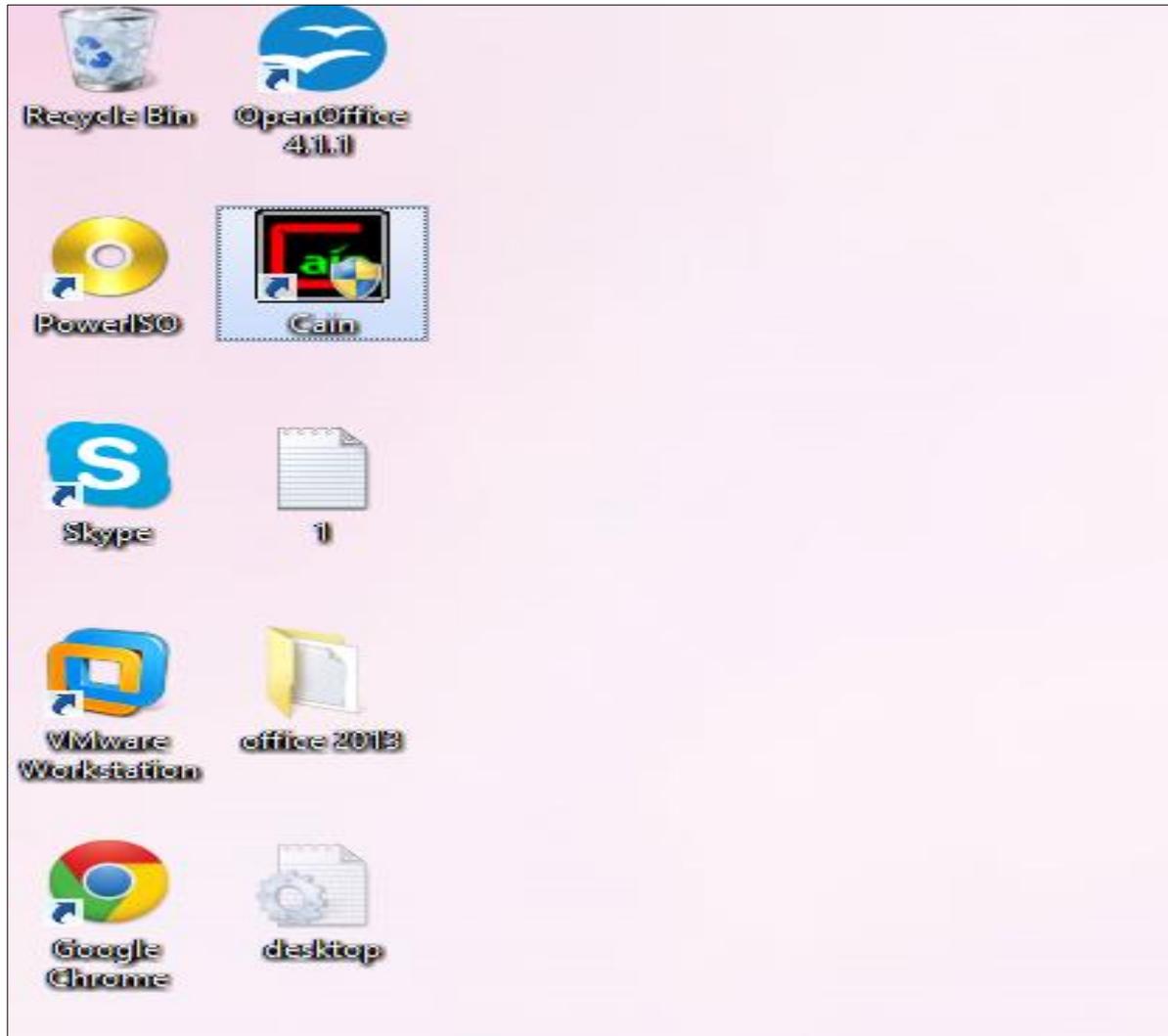


Figure 7: Cain & Abel tool on Windows operating system

**Step 4:** Double click on this icon to open Cain & Abel tool as shown in Figure 8.

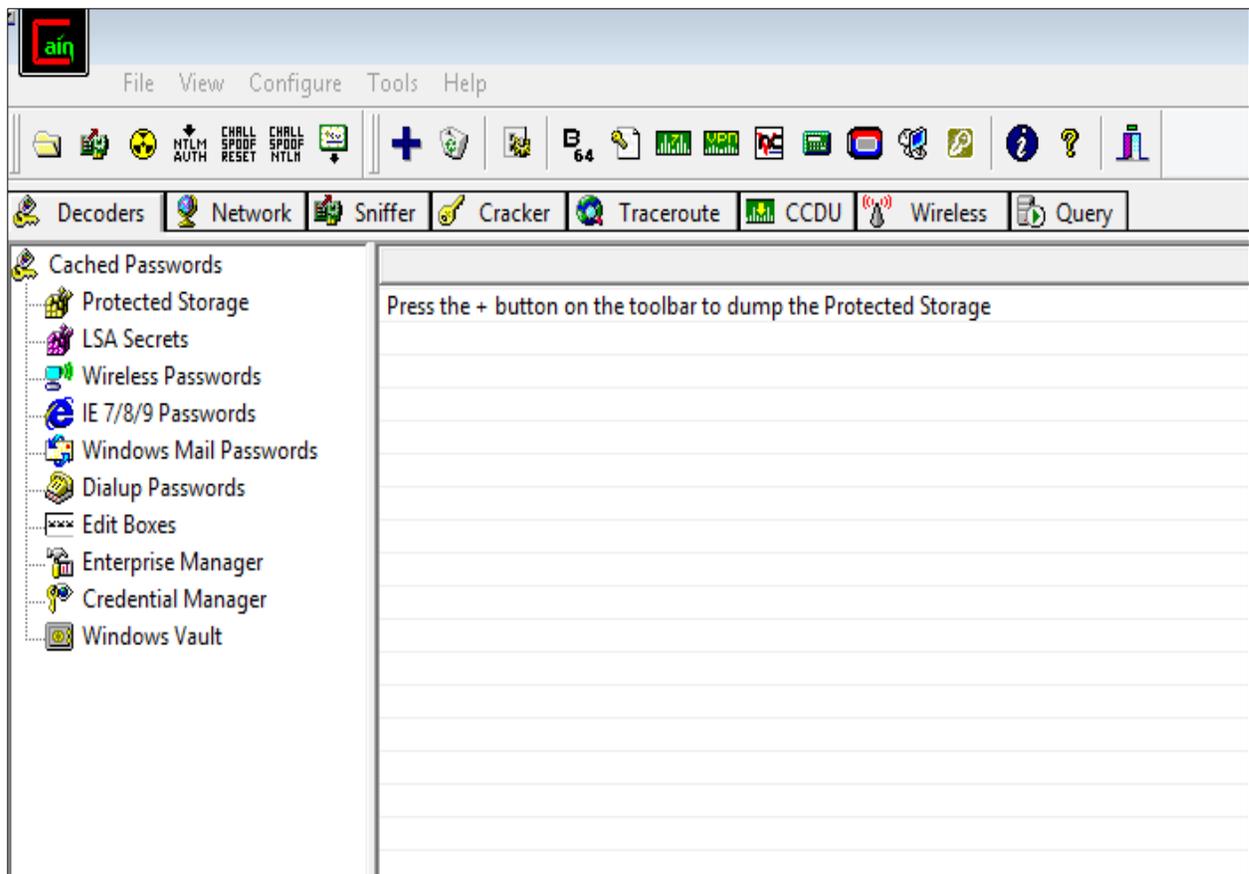


Figure 8: Opening Cain & Abel tool

**Step 5:** Click the sniffer tab and press “configure” to open configuration dialog. Select an adapter from the configuration dialog box and click “ok” as shown in Figure 9.

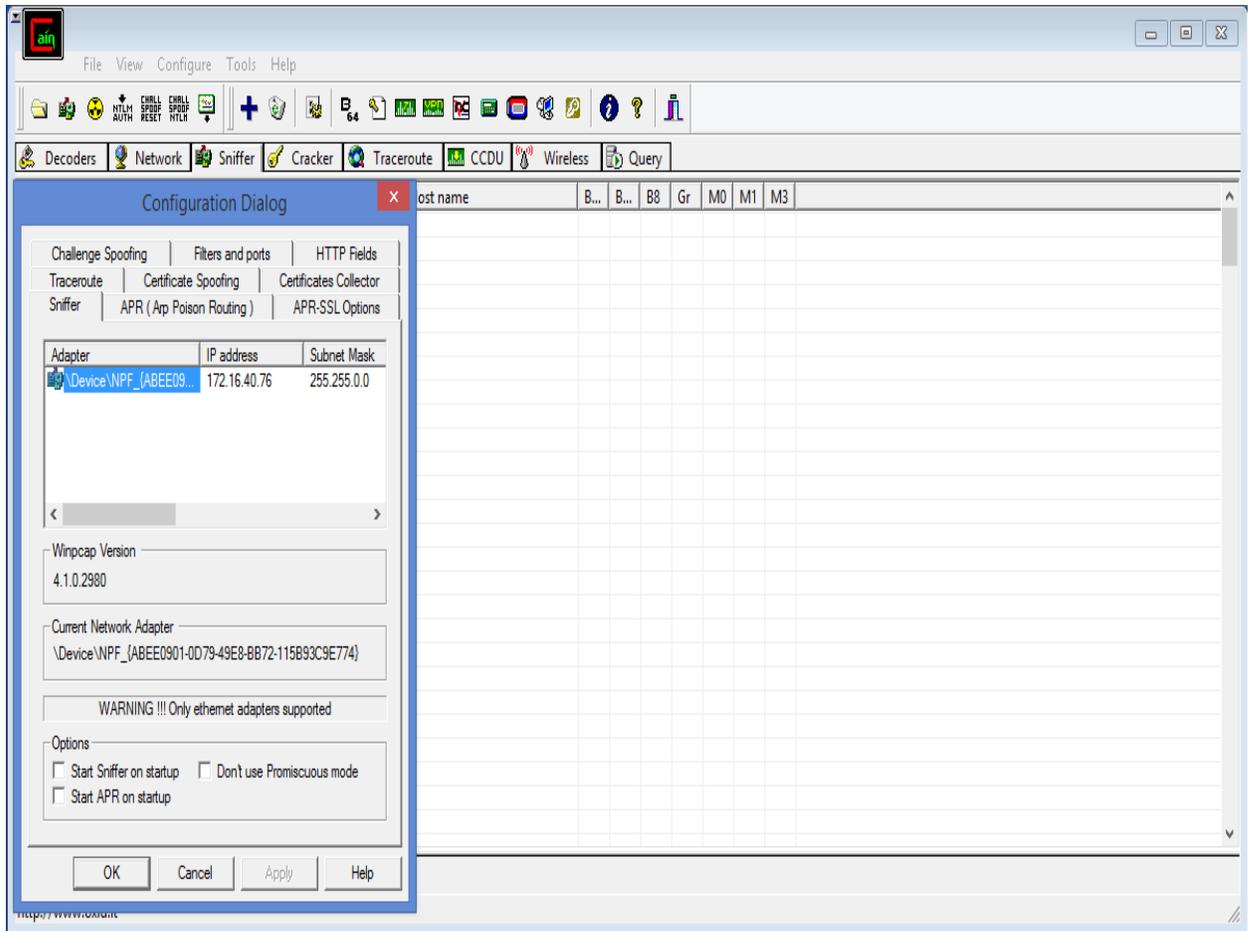


Figure 9: Opening configuration dialog to select the router

**Step 6:** Turn on the sniffer and click the “+” icon to select all host in the subnet or give a range of IP address. Click “ok” as shown in Figure 10.

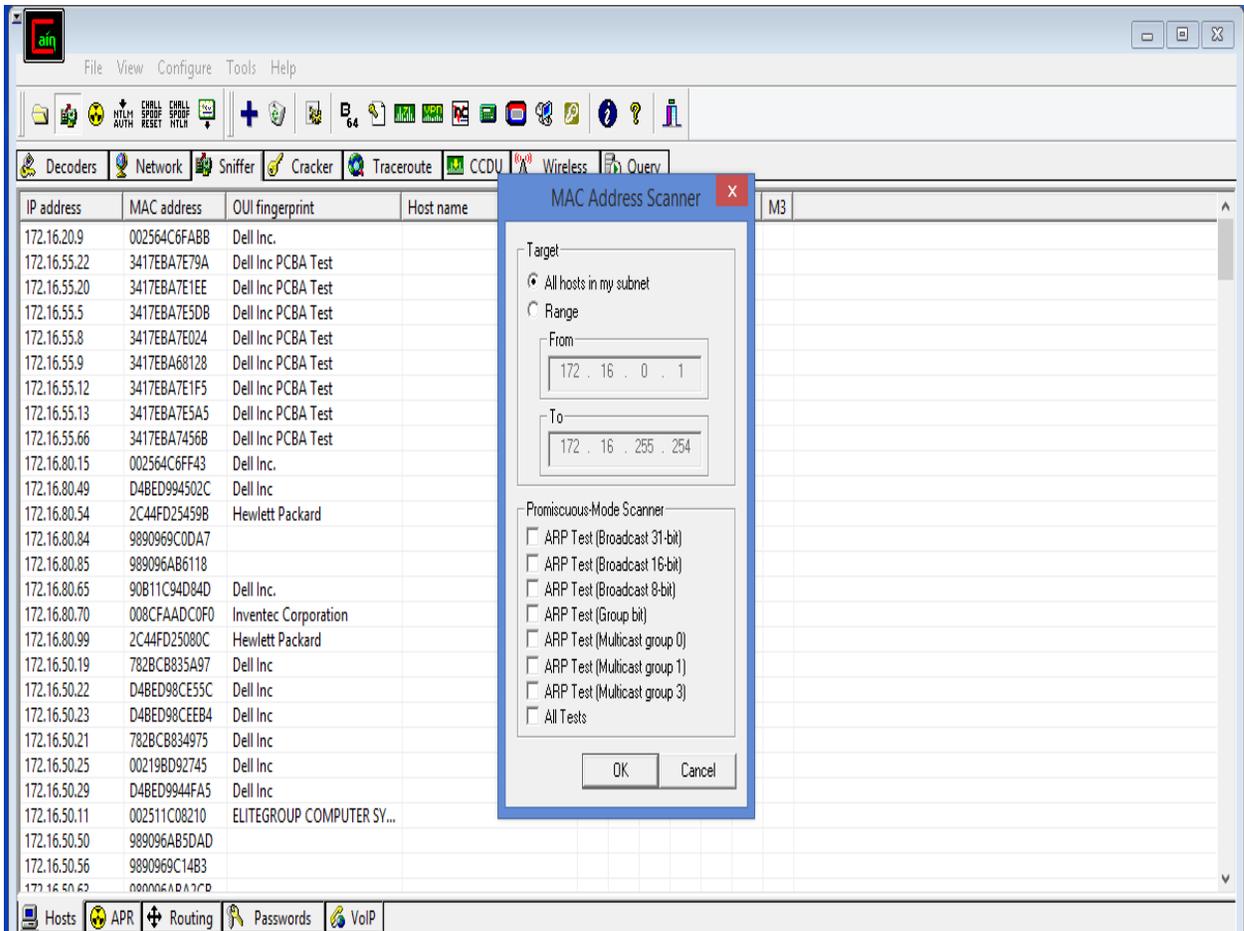


Figure 10: MAC address scanner

**Step 7:** Select the IP address of target host (172.16.55.9) from the list of hosts as shown in Figure 11.

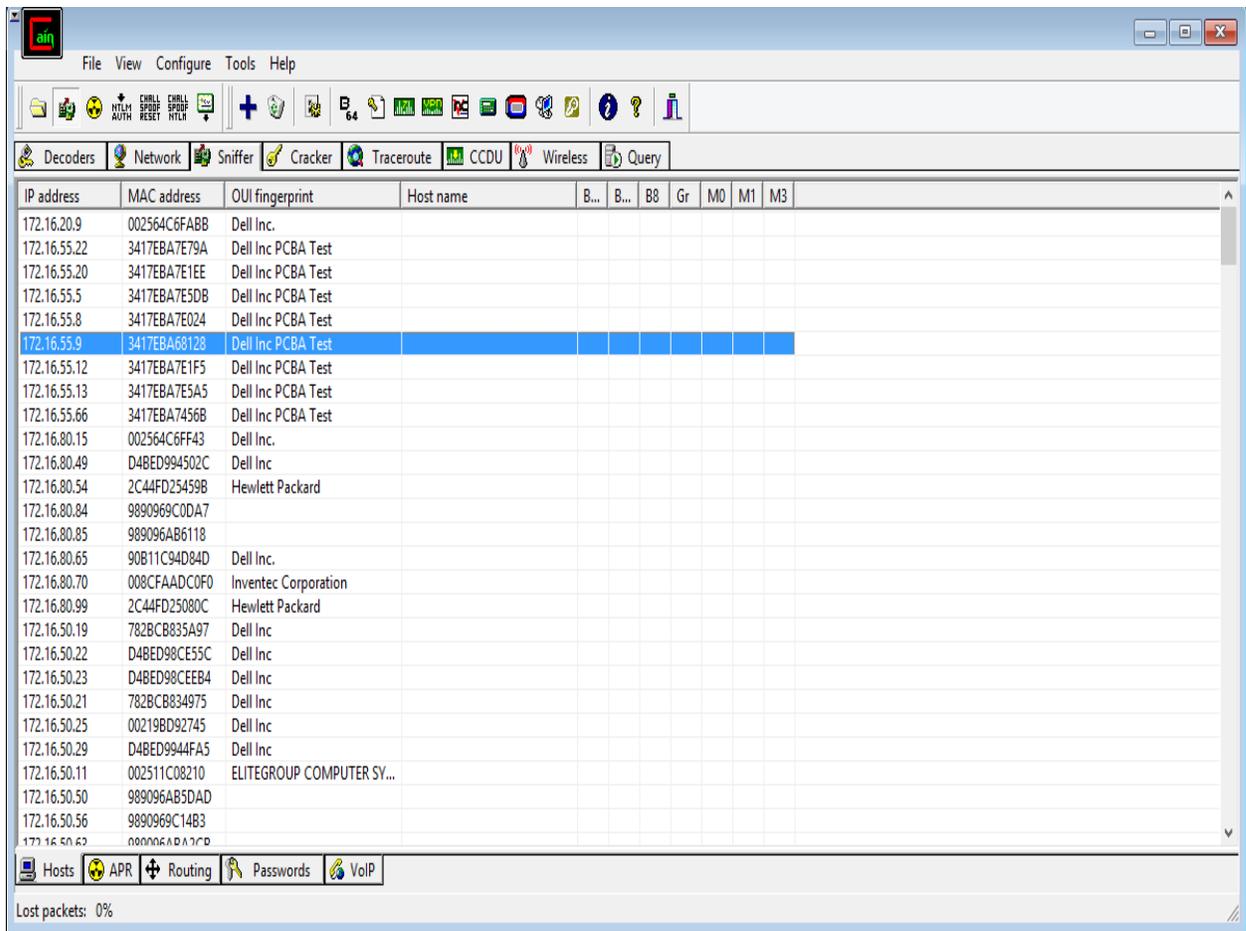


Figure 11: Selecting a target

**Step 8:** Select APR tab and perform ARP route poisoning to poison the route and sniff the network packets. Select the IP address of router on left side of the table and IP address of the target host (or we can select all IP addresses) on the right side of the table as shown in Figure 12 and Figure 13 respectively.

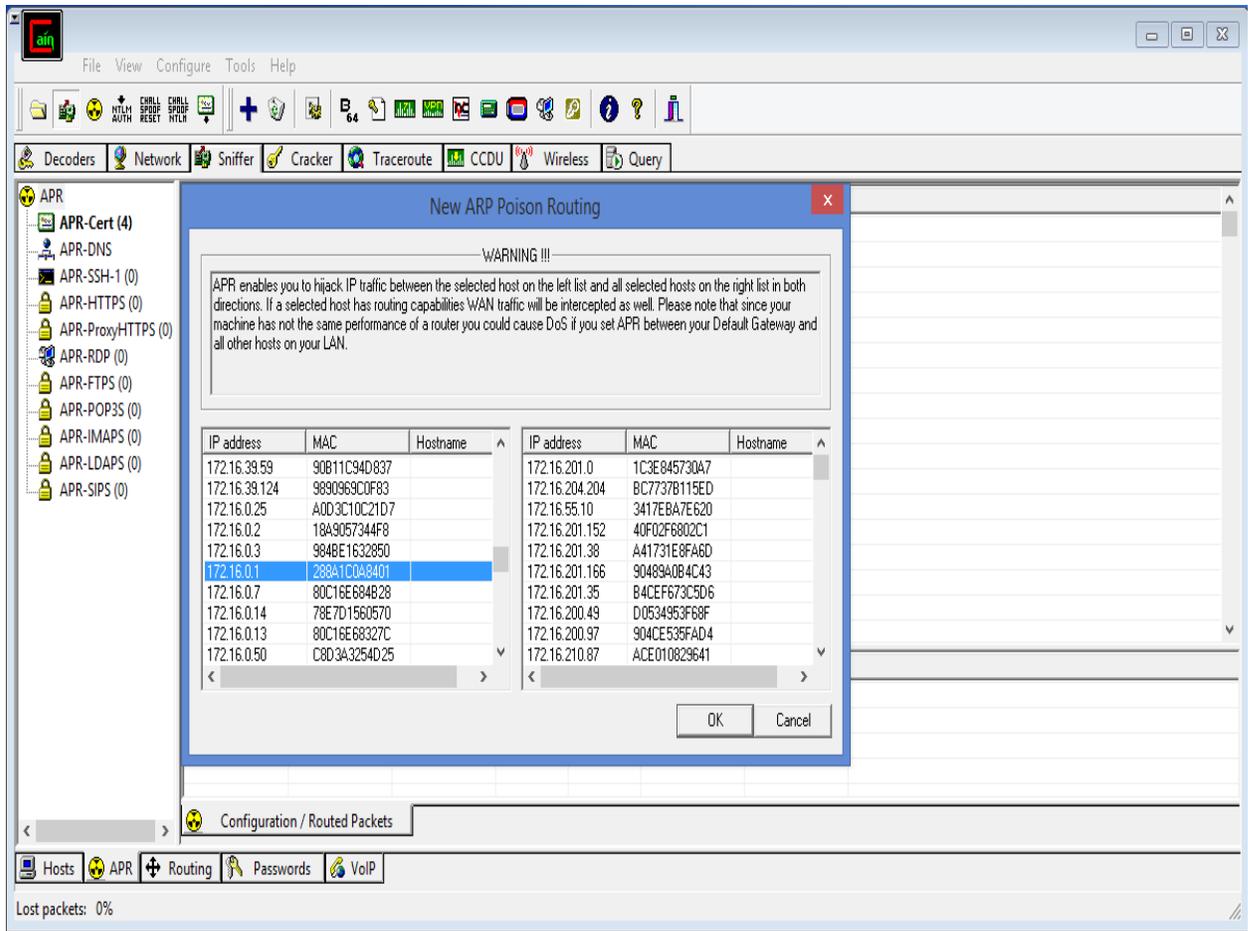


Figure 12: ARP route poisoning

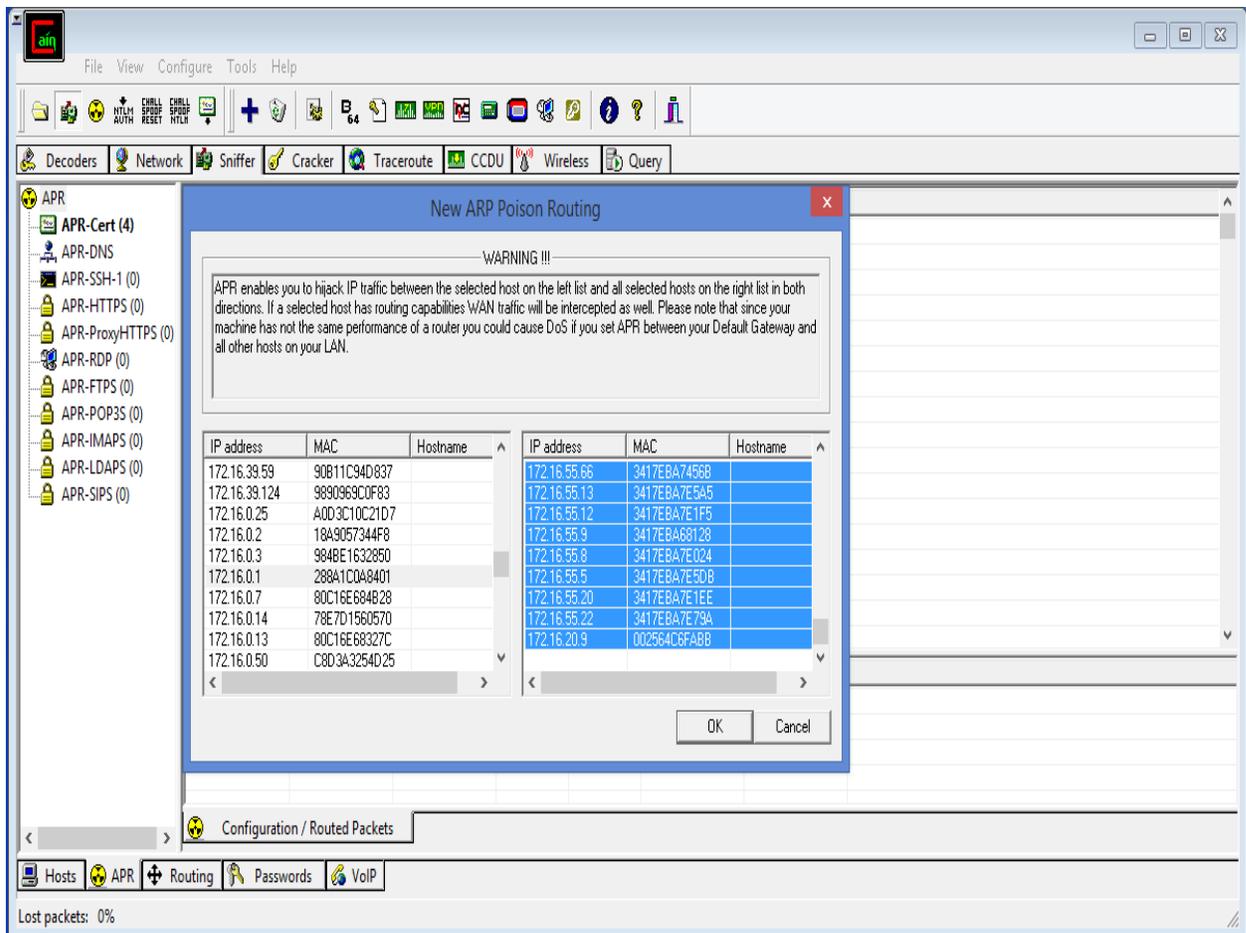


Figure 13: Selecting IP address of router and target host

**Step 9:** As shown in Figure 14, the IP address of the target host (172.16.55.9) is displayed with the IP address of the router (172.16.0.1)

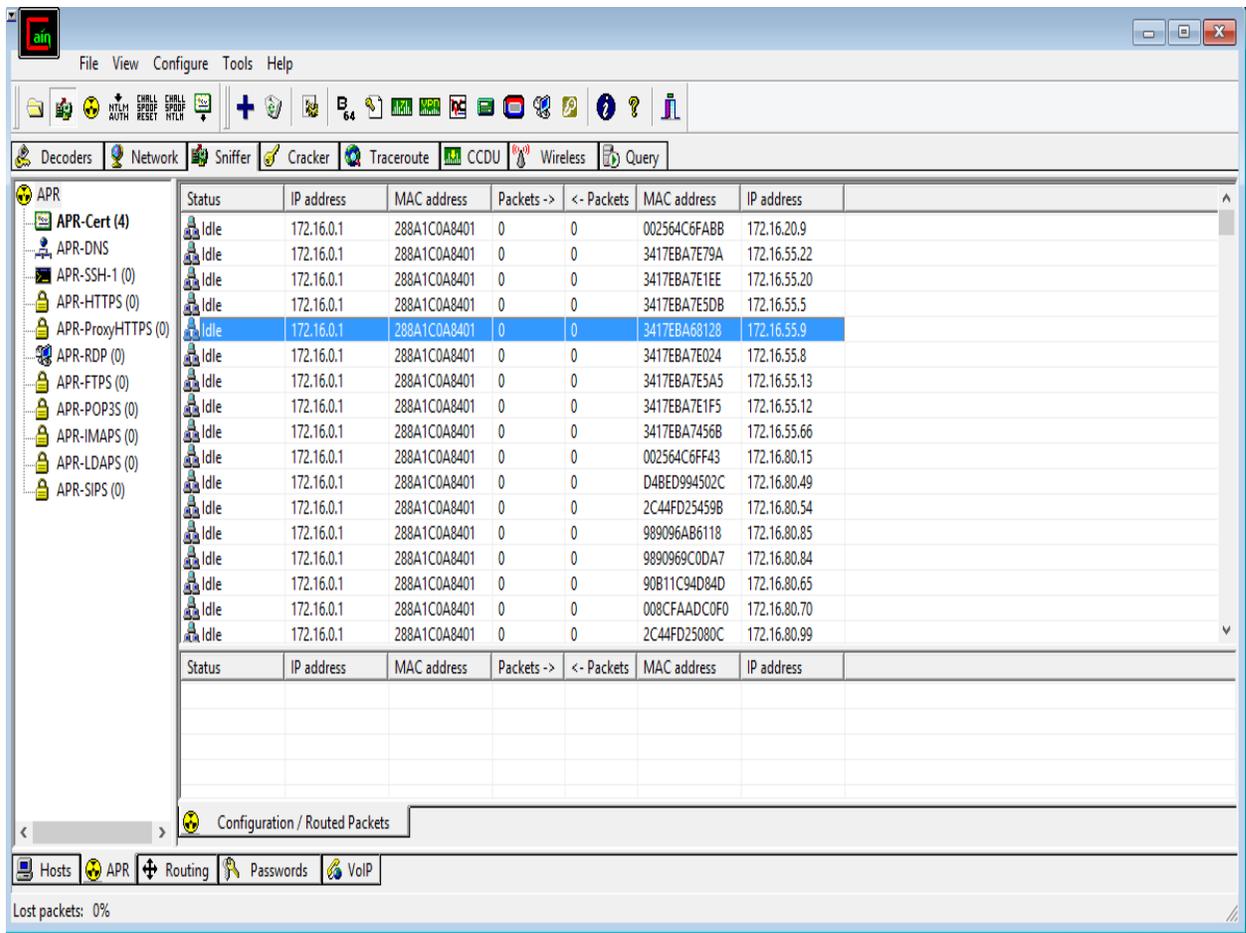


Figure 14: Idle status

**Step 10:** Now open an HTTP website on the target host machine (172.16.55.9) and create an account on that website as shown in Figure 15 and Figure 16 respectively.

hackforums.net/index.php

Welcome to HackForums.net Current time: 10-26-2015, 04:44 AM

# Hack Forums Packets, Punks, and Posts™

[Home](#)
[Upgrade](#)
[Search](#)
[Members](#)
[Extras](#)
[Wiki](#)
[Help](#)
[Follow](#)
[Contact](#)

Hello There, Guest! ([Login](#) — [Register](#))

**Hack Forums**

[Common](#)
[Hack](#)
[Tech](#)
[Code](#)
[Game](#)
[Groups](#)
[Web](#)
[GFX](#)
[Market](#)
[Money](#)

### Hack Forums Official Information

Forum	Threads/Posts	Last Post
<b>Rules, Announcements, News, and Feedback</b> This is where site rules and important announcements about the site are made. Please read carefully before you join. Also you can leave us feedback or ask site questions here. Moderated By: Mentors <ul style="list-style-type: none"> <li><a href="#">Suggestions and Ideas</a></li> <li><a href="#">Wiki Talk</a></li> </ul>	44,093 598,400	<b>Server Move and Bugs</b> Today 04:39 AM by Fourteen

### Hack Forums Open Discussion

Forum	Threads/Posts	Last Post
<b>The Lounge</b> For great discussions on various subjects and to have some fun relaxed topics you can enter our Lounge. Read the rules in the forums as trolling, spamming, or flaming are not allowed. Moderated By: Mentors <ul style="list-style-type: none"> <li><a href="#">Sports World</a></li> </ul>	440,895 6,250,790	<b>HF, what Anti-Virus do yo...</b> Today 04:43 AM by bigwoo
<b>Personal Life</b> Our personal life topics sections are all under subforums of this category. <ul style="list-style-type: none"> <li><a href="#">Education Nation</a></li> <li><a href="#">Health Wise</a></li> <li><a href="#">Bragging Rights</a></li> </ul>	47,509 671,100	<b>I woke up with this!</b> Today 04:44 AM by Truth Hurts

Figure 15: Open an HTTP website on target host

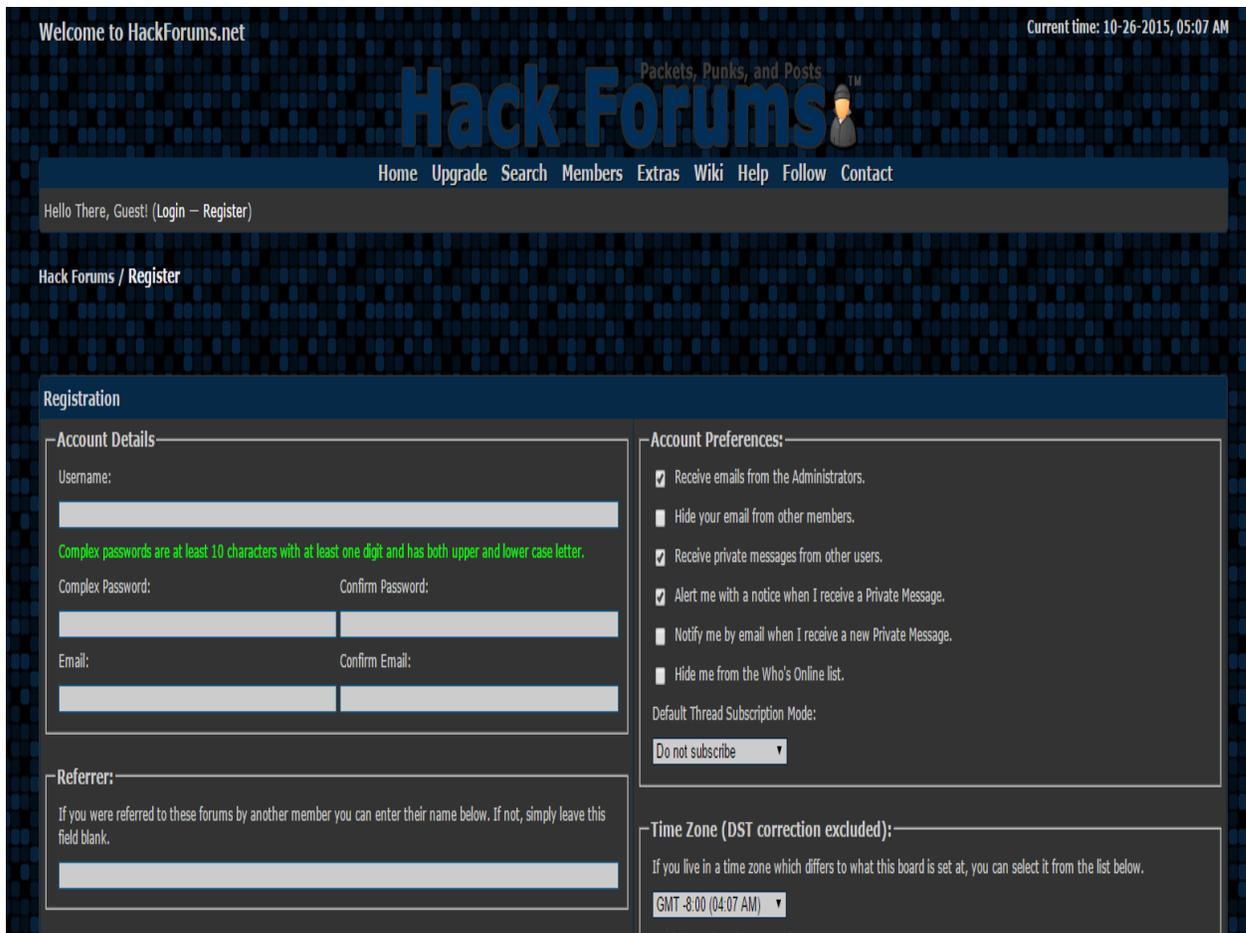


Figure 16: Creating an account in the website

**Step 11:** Now start poisoning the route to sniff the network packets by clicking the APR icon and the status will be changed from “Idle” to “Poisoning” as shown in Figure 17 and Figure 18 respectively.

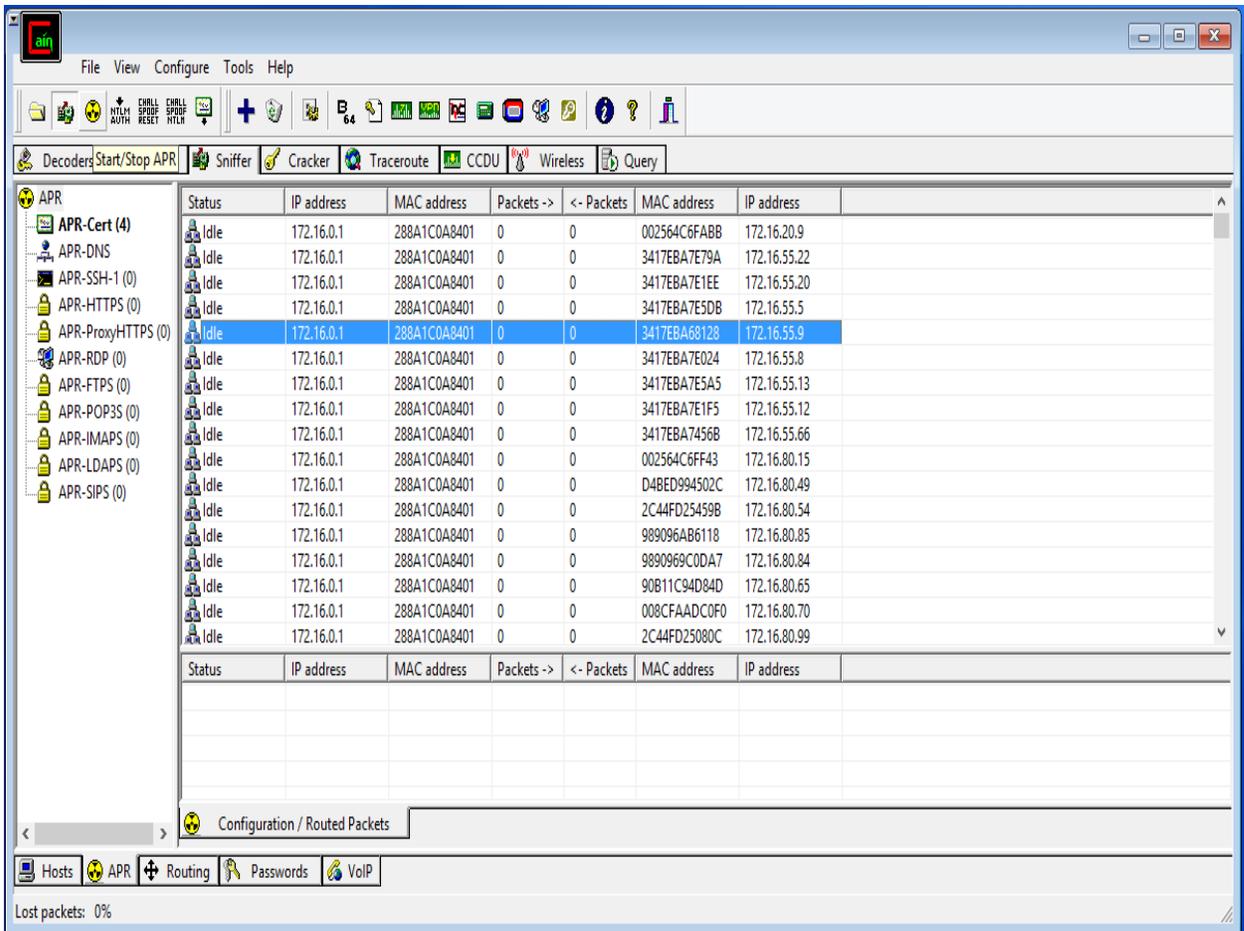


Figure 17: Before poisoning the route

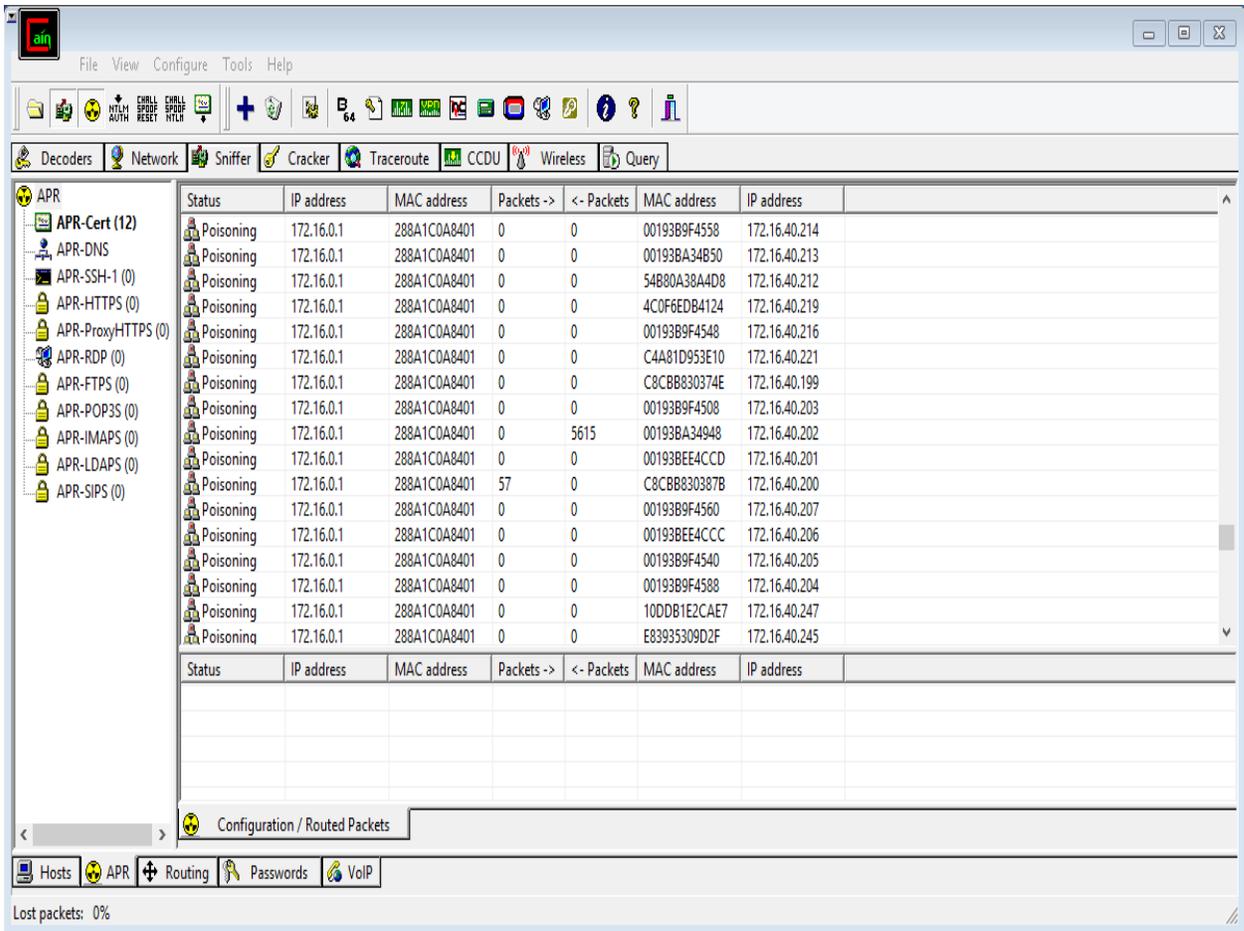


Figure 18: After poisoning the route

**Step 12:** Select “HTTP” tab to check the username, password, and URL captured after sniffing the network as shown in Figure 19 and Figure 20 respectively.

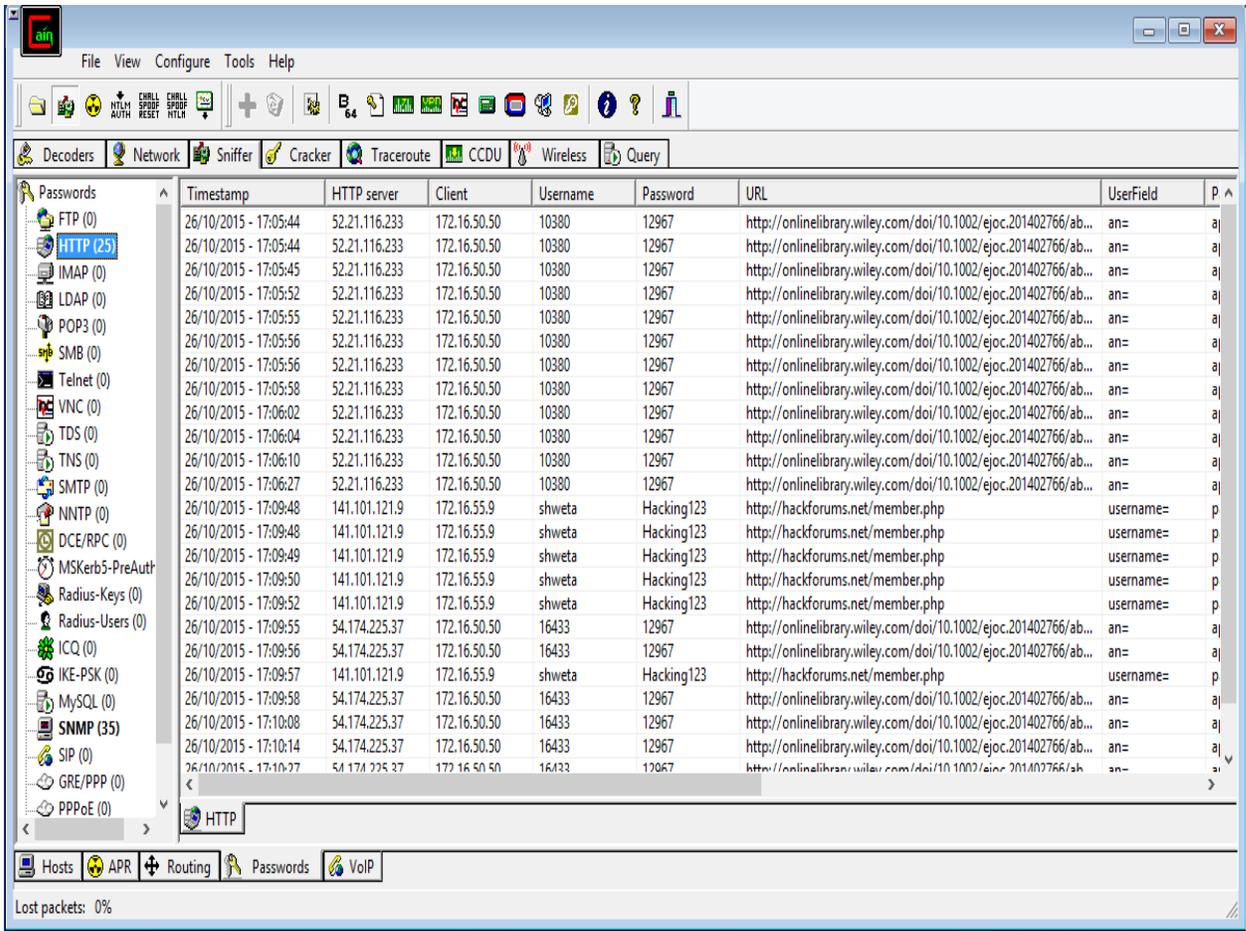


Figure 19: Selecting HTTP tab

Timestamp	HTTP server	Client	Username	Password	URL	UserField
26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:45	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:52	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:55	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:05:58	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:06:02	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:06:04	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:06:10	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:06:27	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:49	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:50	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:52	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:55	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:09:56	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:09:57	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=
26/10/2015 - 17:09:58	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:10:08	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:10:14	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=
26/10/2015 - 17:10:27	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab...	an=

Figure 20: Captured username and password on host machine

**Step 13:** Now login the website with captured username and password on your host machine as shown in Figure 21 and Figure 22 respectively.

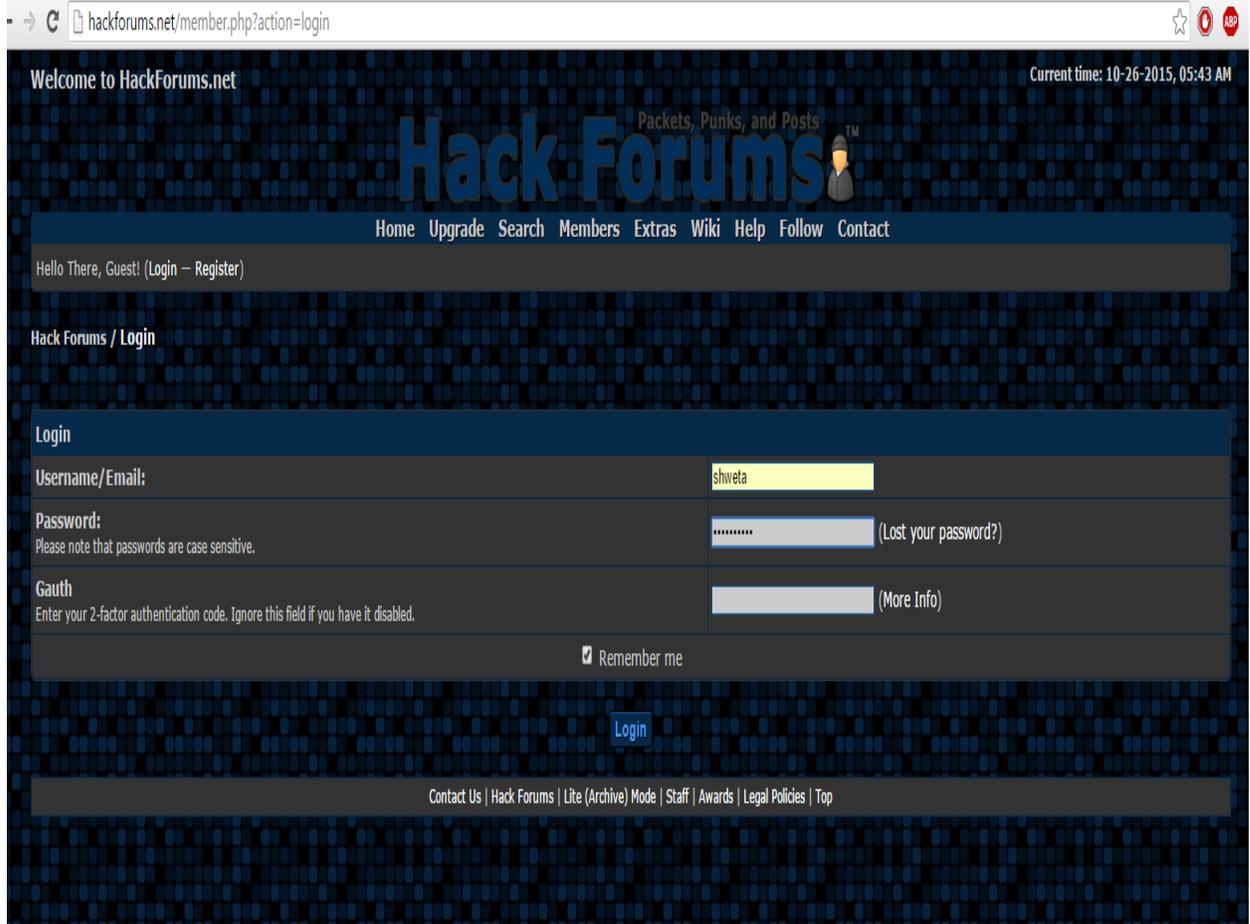


Figure 21: Typing the captured username and password

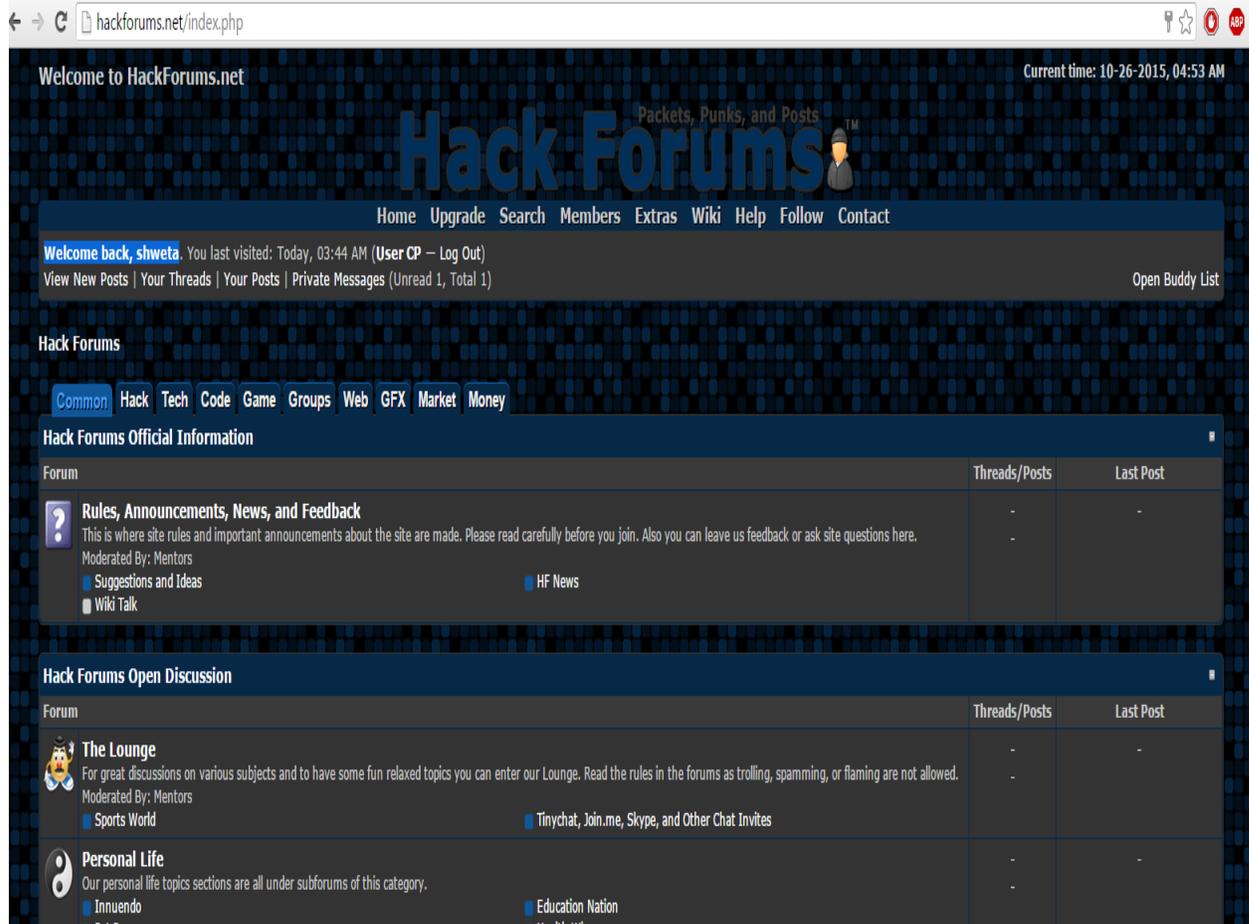


Figure 22: Successfully authenticated

## COUNTERMEASURES

The following countermeasures must be followed to prevent sniffing of usernames and passwords:

- **Use HTTPS websites:** Always make account on HTTPS website. In HTTPS, 'S' stands for security which implies the passwords are stored in encrypted form.
- **Don't make accounts in HTTP websites:** The passwords stored in HTTP websites are in plain text and are not

encrypted. That's why they are easily readable by the hackers.

- **Wrong Policy:** While developing a website, an error message of wrong username should not be displayed as "incorrect username" as shown in Figure 23 because hackers can get an idea that the password is correct while the user name is incorrect. Similarly, an error message of wrong password should not be displayed as "incorrect password" as shown in Figure 24 and Figure 25 because hackers can get an idea that the password is incorrect while the username is correct.
- **Correct policy:** The correct policy of showing an error message is- "incorrect username or password" as shown in Figure 25. This will increase the permutation and combination computations of hackers because they need to spend more time to get the username and password.

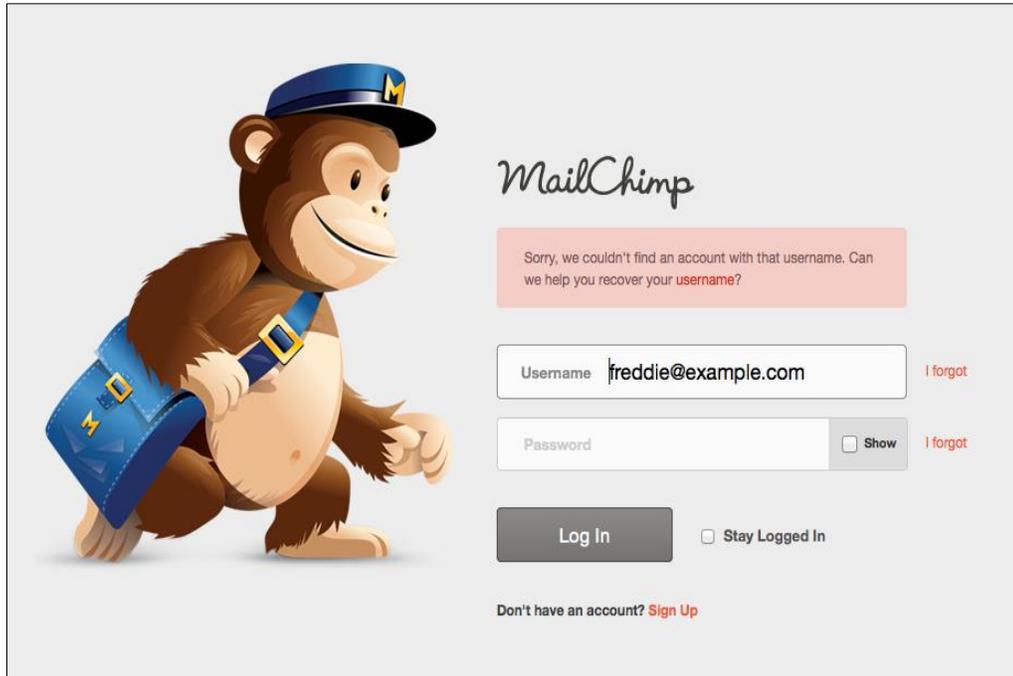


Figure 23: Wrong policy-I



Figure 24: Wrong policy-II

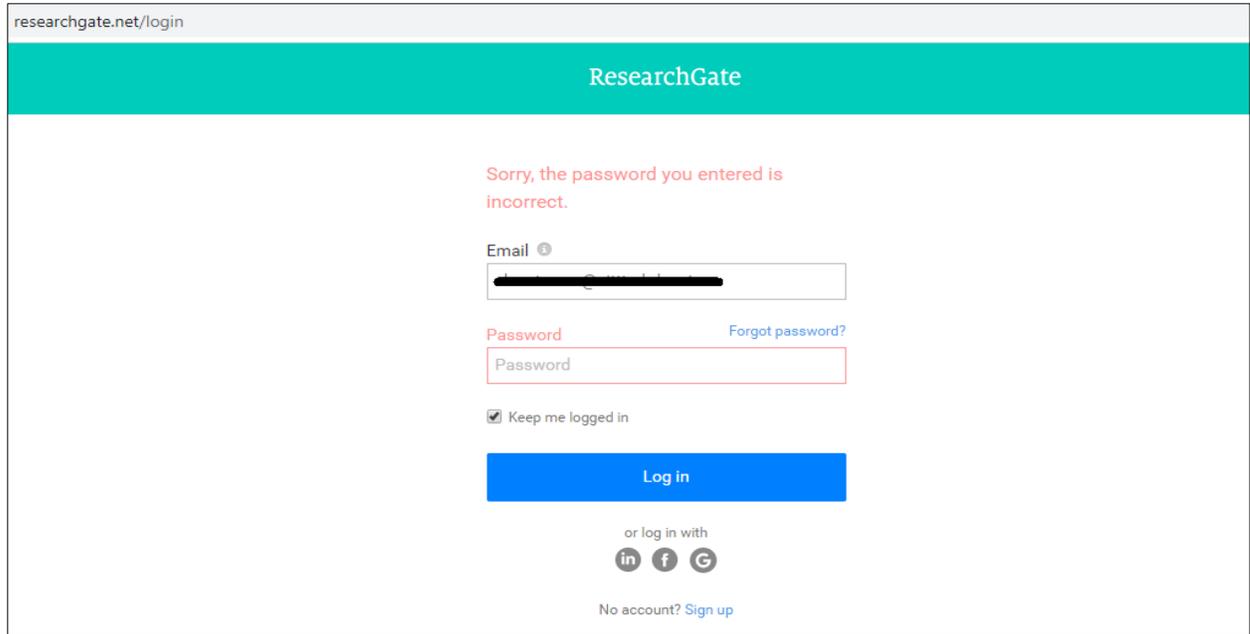


Figure 25: Wrong policy-III

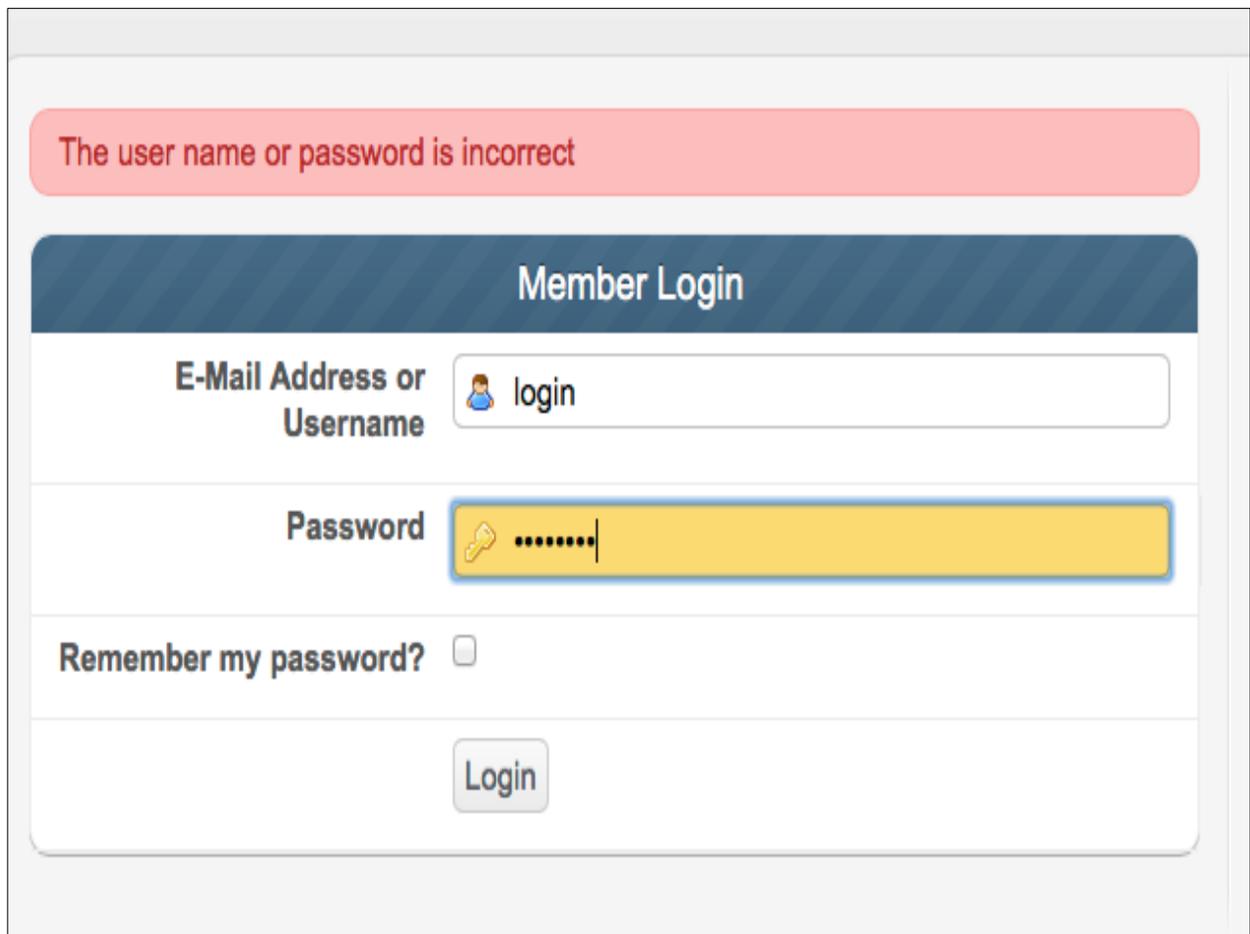


Figure 25: Correct policy

# REFERENCES

- [1] Darknet, "Cain And Abel Download – Windows Password Cracker," 2017. <https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-password-cracker/> (accessed Apr. 11, 2020).