ایران ویج

مجله الکترونیکی ایران ویج

شماره سوم | آذر ۹۱

iranled.com/forum

رمز کردن اطلاعات

معرفی IDE های php و python

کارگاه عملی mac-flood با روتر سیسکو

پروژه مهرامین (شمارنده تعداد رکعت و سجده در نماز)

ساعت led

مثال عملی اندازی گیری اعداد منفی با lm35

فهرست

رمز کردن اطلاعات ۱
مروری بر محیط های توسعه php ٤

پیاده سازی حملات mac-flood ۷
مجموعه آموزشهای پایتون (قسمت اول - eclipse) ۱۵

پروژه مهر امین ۱۹
ساعت led ۲۰

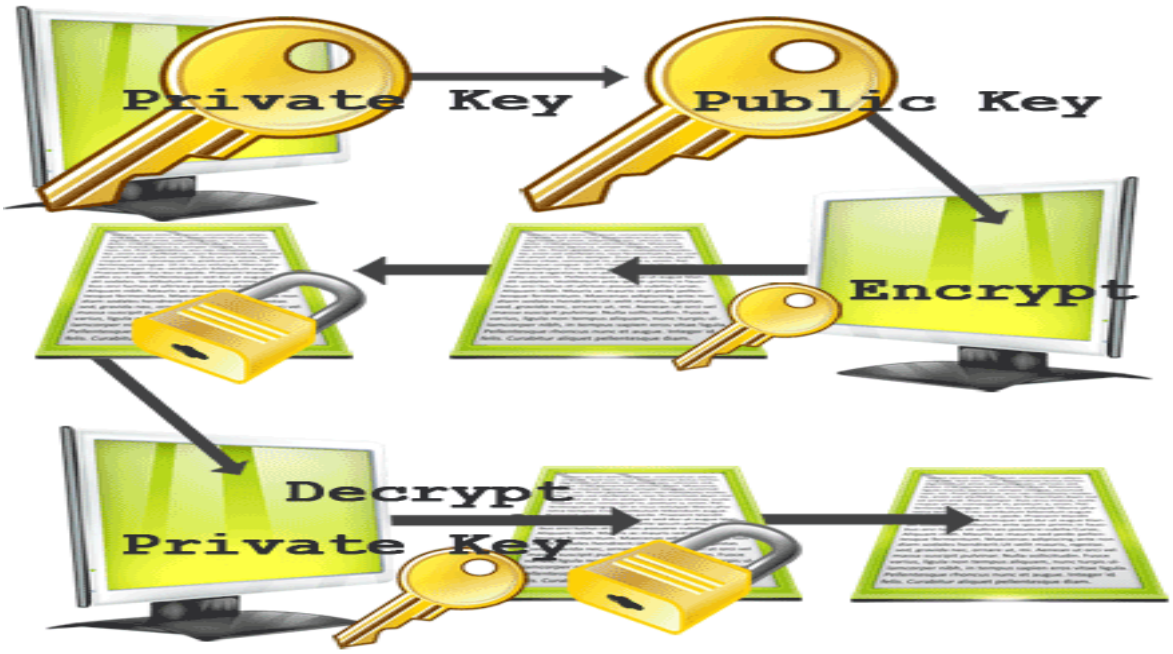
طریقه اندازه گیری دمای منفی با lm35 ۲۱

نویسندگان :

lord_viper
AHA (godvb)
hadikh73
r0b0

طراح جلد و صفحه آرایی :

babyy



رمز کردن اطلاعات

نویسنده :
lord_viper

امروزه یکی از مهمترین بخشهای امنیت در کامپیوتر مقوله رمزنگاری داده ها میباشد رمزنگاری باعث اطمینان از در امان ماندن محتوی اسناد در مقابل عوامل خارجی میباشد

روشهای مختلفی برای رمز نگاری وجود که عبارت اند

۱. کد کردن اطلاعات: کدینگ یا در هم ریزی دادها روشی برای غیر قابل خوانا کردن فایلها و نوشته ها میباشد که معمولا از یک الگوریتم تشکیل میشود مانند rot13
۲. انکریپت کردن: اطلاعات با استفاده از حداقل یک کلید و الگوریتمهای خاصی تغییر داده میشوند که همیشه از ۲ الگوریتم در ان استفاده میشود یکی برای انکریپت و دیگری برای دیکریپت مانند 3des
۳. هش کردن: در این روش اطلاعات با استفاده از الگوریتمهای خاصی تبدیل به یک چکیده با طول خاص میشوند مثلا ۱۲۸ یا ۲۵۶ بایت کمتر یا بیشتر (بسته به نوع الگوریتم) مانند md5

چه دلایلی براس استفاده از این الگوریتم ها وجود دارد ؟

۱. وقتی که می خواهید مطمئن باشید که ایمیلی را که می‌فرستید تنها گیرنده‌ی مورد نظر می‌تواند بخواند؛ و در بین راه ارسال یا حتی پس از دریافت برای کس دیگری قابل خواندن نباشد.
۲. وقتی می‌خواهید اطلاعات خاصی را (نوشته، عکس و یا ویدئو) تنها برای خود یا فرد خاصی قابل دسترسی کنید.
۳. وقتی می‌خواهید یک گروه درست کنید و از شنود افراد غیر مجاز در امان باشید. در واقع، ابداع‌کننده‌ی اصلی این روش، یعنی فیل زیمرمن، از فعالان ضدهسته‌ای در ایالات متحد بود که برای تدارک دیدن تظاهرات و کارشکنی در انتقال مواد هسته‌ای نیاز به حذف شنود FBI داشت.
۴. وقتی نگران هستید که اطلاعات و محتوای ایمیل‌تان توسط شرکت‌های فراهم‌آورنده‌ی ایمیل مجانی برای تهیه‌ی یک پروفایل تجاری از شما و هدف‌گیری تبلیغاتی‌تان - و نیت‌های شوم دیگر استفاده شود.
۵. وقتی می‌خواهید مطمئن شوید نویسنده یا تولید کننده‌ی یک مطلب حتماً همان کسی است که ادعا می‌کند.
۶. وقتی روزانه تعداد زیادی ایمیل و اسپم دریافت می‌کنید، می‌توانید بگویید تنها به ایمیل‌هایی جواب می‌دهید که رمز شده باشند (این کاری است که مخترع WWW، یعنی Sir Tim Berners Lee و تعدادی دیگر از همکاران‌اش در Cern انجام داده‌اند). سرورهای فرستنده‌ی اسپم به دلیلِ هزینه‌ی محاسباتی رمز نگاری نمی‌توانند ایمیل رمز شده بفرستند.

همانگونه که در بالا گفته شد روشهای مختلفی برای رمز نگاری اطلاعات وجود دارد که یکی از ساده ترین روشها کد کردن اطلاعات میباشد دارد مثلا کلمه hello را یک حرف به جلو شیفت میدهم در این حالت حرف o از انتها به ابتدای کلمه منتقل خواهد شد و به صورت زیر در خواهد آمد elloh یا مثلا هر حرفی با حرف بعد از خود جایگزین شود در این حالت کلمه hello به صورت ifmmp در خواهد آمد.

الگوریتمهای مختلفی برای این کار وجود دارد که عمومی ترین آنها

Xor – rot13 – Base64

میباشد که در این مقاله به پیاده سازی اینها میپردازیم

XOR

در این روش متن مورد نظر را با یک مقدار XOR میکنیم همانطور که میدانید XOR یک عملگر منطقی میباشد

Boolean XOR		
Operands		Result
false	false	false
false	true	true
true	false	true
true	true	false

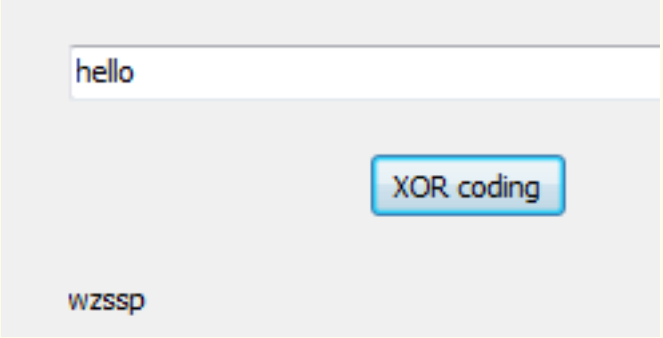
درجدول فوق شرط درستی در حالتی است که حتما یکی از المانها غلط False یا 0 باشد

حالا به پیاده سازی الگوریتم فوق میپردازیم؛ در ابتدا یک پروژه جدید ایجاد و یک Label-Edit-button بر روی فرم قرار میدهیم و در رویداد Onclick دکمه کد زیر را مینویسیم (کد شماره ۱)

```
procedure TForm1.btn_xorClick(Sender: TObject);
var
        ch,ci:Char;
        str,val:string;
begin
        str:=edit1.Text;
        for ch in str do
        begin
                ci:=chr(Ord(ch)xor 31);
                val:=val+ci;
        end;
        label1.Caption:=val;
end;
```

(کد شماره یک)

تابع ord مقدار یک حرف(کاراکتر) را به مقدار معادل عددی ان در استاندارد ASCII تبدیل میکند و تابع chr هم یک مقدار عددی را به مقدار کاراکتر معادل ان در استاندارد ASCII تبدیل میکند ما در این الگوریتم مقدار هر کاراکتر را با عدد ۳۱ عمل xor انجام میدهیم در این حالت مقدار رمز شده کلمه hello به صورت wzssp خواهد بود



ROT13

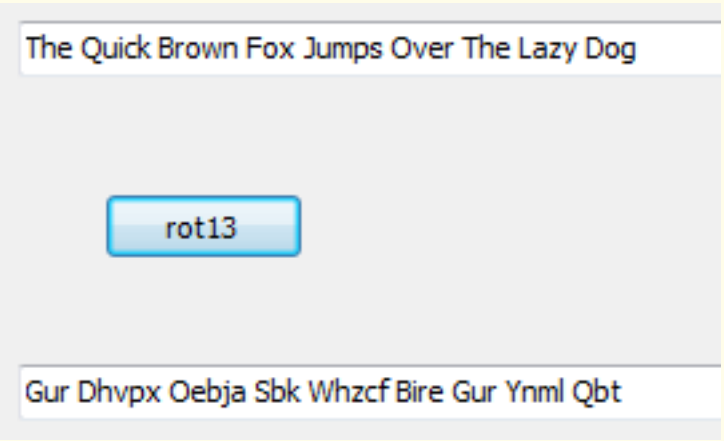
همانطور که میدانید زبان انگلیسی دارای ۲۶ حرف میباشد (عدد ۱۳ از تقسیم تعداد حروف؛ بخش بر ۲ حاصل میشود). ROT هم به معنی rotate یا گردش میباشد در این الگوریتم حروف بزرگ و کوچک به ۲ دسته ۱۳ تایی تقسیم میشوند از A-M a-m و N-Z n-z تقسیم میشوند اگر مقدار عددی ASCII یک حرف در گروه اول باشد مقدار آن با ۱۳ جمع میشود اگر مقدار عددی ASCII یک حرف در گروه دوم باشد مقدار ان از ۱۳ کم میشود به مثال زیر توجه کنید

```
function rot_encode(val: string; num: Integer):
string;
var
        ch: Char;
        i: Integer;
        str: string;
begin
        str := '';
        for ch in val do
        begin
        if (ch in['a'..'m'])or (ch in['A'..'M']) then
اگر مقدار کاراکتر ch در گروه اول A-Z, a-m باشد مقدار آن با 13 جمع میشود
                i:=ord(ch)+13
        else
        if(ch in['n'..'z'])or(ch in['N'..'Z'])then

اگر مقدار کاراکتر ch در گروه اول N-Z, n-z باشد مقدار آن با 13 جمع میشود

                i:=ord(ch)-13
        else
                i:=Ord(ch);
                str:=str+chr(i);
        end;
        result := str;
end;
```

(کد شماره دو)

روش استفاده

```
edit2.Text := rot_encode(edti1.Text);
```



Base64

base64 از معروفترین کدینگها میباشد که کاربرد زیادی نیز دارد، یکی از مصارف آن انتقال وصله های ایمیلهاست. به دلیل اینکه در پروتکل MIME باید از کاراکترهای اسکی استفاده نمود لذا از این روش کدینگ استفاده می شود(بعضی از کاراکتر های غیر اسکی در این پروتکل معنی خاصی دارند). برای اطلاعات بیشتر، RFC های مربوط به MIME را بخوانید. در بعضی برنامه های تحت وب برای ساختن ادرس صفحات وب از آن استفاده میشود. طراحی و پیاده سازی این الگوریتم بسیار ساده میباشد. طول کدی که در این روش تولید میشود 33% از مقدار اولیه بیشترخواهد بود.

پیاده سازی الگوریتم

base64 دارای 64 سمبل میباشد که از 0 تا 63 شماره گزاری میشوند:

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijkl
mnopqrstuvwxyz0123456789+/

این الگوریتم بر روی بیتها و بایتها اعمال میشود به این صورت که هر متنی از مجموعه حروف تشکیل میشود و در حالت عمومی هر حرف یا هر کاراکتر 1 بایت میباشد و هر بایت 8 بیت میباشد. ولی کاراکترهای استفاده شده در این الگوریتم 6 بیتی میباشد و این رمز نهفته در این الگوریتم میباشد! ابتدا حروف یک عبارت را تبدیل به بایتها و بیتهای متناظر آن میکنیم.

در این مثال فرض کنید کلمه Man را می خواهید به Base64 انکد کنید کلمه Man از 3 حرف M,a,n تشکیل شده است که مقدار ascii آن برابر شماره 77,97,110 در مبنای 10 میباشد حال این اعداد را به مبنای 2 میبریم توجه داشته باشید که حتما در تبدیل باید طول هر کدام 8 بایت شود! برای این کار بعد از تبدیل به مبنای 2 انقدر به اول ان صفر اضافه کنید تا طول ان به 8 برسد. اعداد فوق در مبنای 2 بصورت 01001101, 01100001, 01101110 است حال این بیتها راکنار هم قرار میدهیم تا رشتهای از بیتها بوجود اید:

0 1 0 0 1 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0

با توجه به اینکه 2^6 سمبل داریم پس هر کاراکتر در پایه 64, 6 بیتی می باشد در صورتی که در اسکی کاراکتر ها 8 بیتی هستند

در base64 کاراکترها 6 بیتی میباشند حالا ما رشته را 6 بیت 6 بیت جدا میکنیم و به مبنای 10 میبریم که میشود

19 22 5 46

حالا مقدار این اعداد را از جدول base64 میخوانیم که میشود

T W F u

حال اگر تعداد کاراکترها 5 عدد باشد طول رشته 40 میشود که در این مبنا 6 کاراکتر میشود و برای کاراکتر بعدی 2 بیت کم می اید در اینجا باید 4 بیت را به مبنای 10 برده و مقدار را از جدول بخوانیم و به ازای هر 2 بیت که داریم یک = قرار میدهیم

برای مثال sazan در base64 بصورت c2F6YW4= میشود. برای دیکود کردن هم کافی است همین روند را از انتها به ابتدا دنبال کنید. البته این الگوریتم در خود زبان دلفی در یونیت Soap.EncdDecd قرار دارد و به سادگی با uses کردن آن و استفاده از توابع زیر این کار را انجام دهید

```
EncodeString(val:string):string;
DecodeString(val:string):string
```

مثال:

```
showmessage(EncodeString('lord_viper'));
```

مقدار کد شده عبارت lord_viper برابر با bG9yZF92aXBlcg== خواهد بود و برای دیکود به صورت زیر عمل کنید

```
showmessage(DecodeString('bG9yZF92aXBlcg=='));
```

دو نمونه سورس کد با نام های :

Decode
EncodeBase64

همراه پیوست مجله در پوشه delphi موجود است.

مروری بر محیط های توسعه php

phpDesigner8

نویسنده:

lord_viper

ide های زیادی برای کار با php وجود دارد که هر کدام دارای قابلیتهای کم و زیادی هستند، مثل NuSphere PhpED , dreamweaver, NetBeans IDE, Zend Studio, phpDesigner و .... یکی از محیطهای توسعه (IDE) خوب در این میان phpDesigner میباشد که اخرین نسخه موجود ان ۸،۱ میباشد میتوانید اخرین نسخه این برنامه را از سایت
http://www.mpsoftware.dk
دریافت کنید.

این محیط دارای قابلیتهایی مانند Code complatation شامل html5- css3-javascript و php5, php4 میباشد

Debugger:یک خطا یاب برای php که اشتباهات کدنویسی را به شما اعلان میکند

Code beutifuler:فرورفتگی و برامدگی در کد ایجاد میکند تا خوانایی کد بالاتر رود

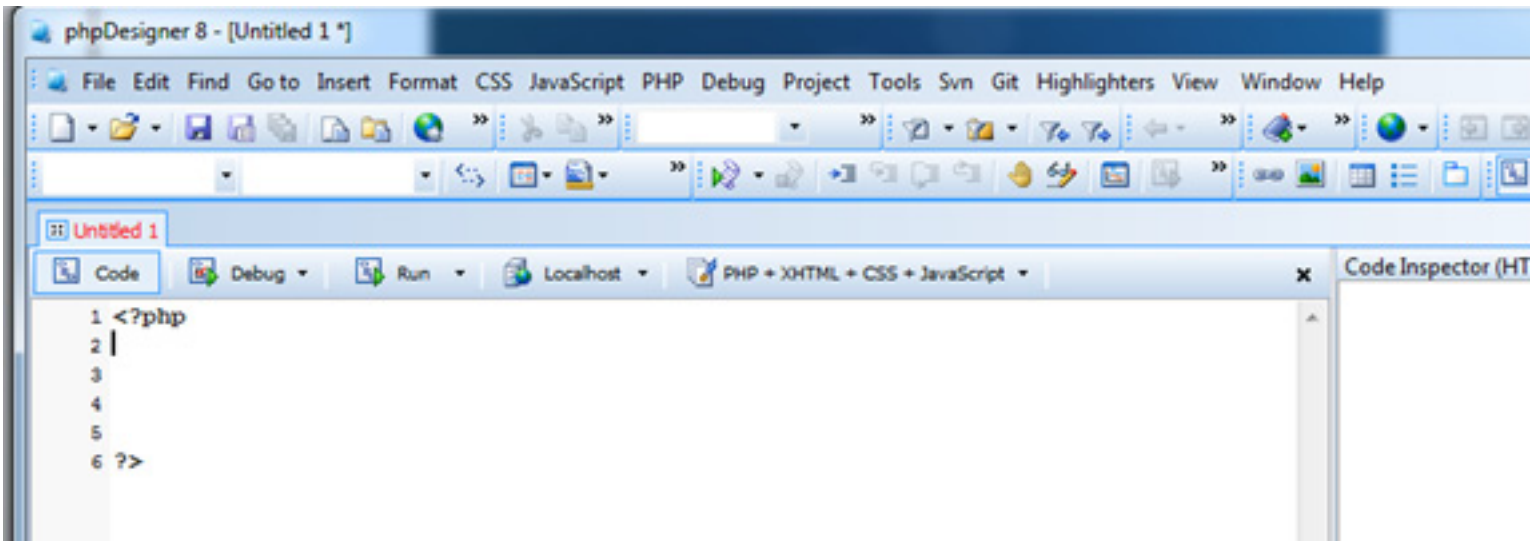
Line number: ادیتور ان هر خط کد را شماره گذاری میکند

Svn:قابلیت کار با سرورهای svn را دارا میباشد

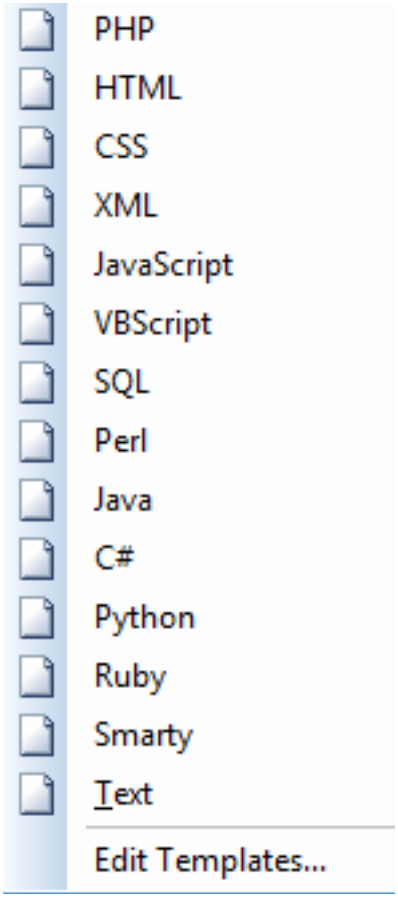
ftp:ابزارهای لازم برای کار با ftp و اپلود سایت بر روی سرور در ان گنجانده شده است

و خیلی بخشهای دیگر با حجم ۲۴ مگ میباشد.این محیط از ۴ بخش اصلی تشکیل شده است

۱. منو:این قسمت دارای بخشهای متنوعی میباشد مانند - insert - highlight - tools - debuge - php - javascript و ...
۲. جعبه ابزار:ابزارهای مورد نیاز برای دسترسی سریعتر روی ان قرار دارد مانند run-debuge-open-new
۳. ویرایشگر:دارای یک ویرایشگر خوب که نیازهای یک برنامه نویس برای شروع را رفع میکند
۴. پنجره مدیریت:این بخش خود شامل چند سربرگ مجزی شامل ode explorer - code inspector (html) - file browser - projects - ftp/ sftp - themplates - code snipts میباشد



بخش new شامل ایجاد فایلهای زیر میباشد (شکل یک)

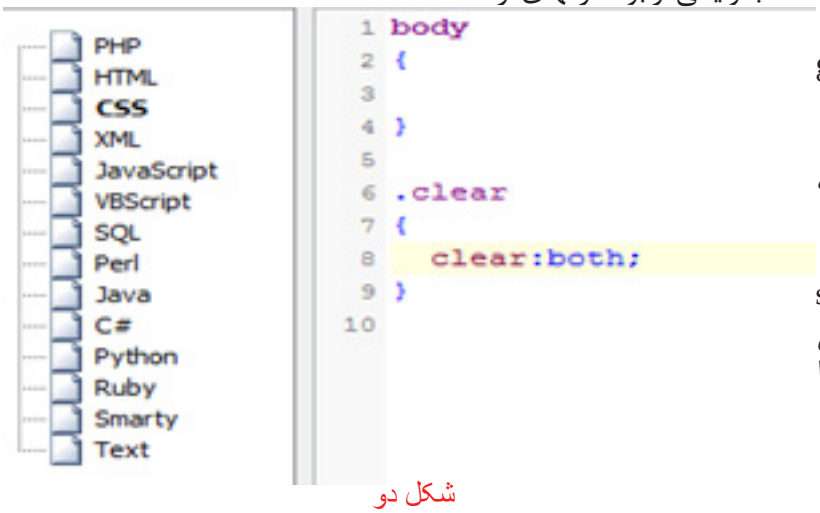


شکل یک

بخش Edit Themplate که از این بخش میتوانید تمپلیت فایل مورد نظر را عوض کنید یا تمپلیت مورد نظر خود را ایجاد کنید مثلا فایلهای css یا پرل دارای هیچ تمپلیتی نمیباشد میتوانید روی css کلیک کرده و این گزینه را انتخاب کنید و در ویرایشگر باز شده کد زیر را قرار داده و close کنید (شکل دو)

حالا اگر یک فایل css باز کنید این تمپلیت به صورت پیشفرض در ان قرار دارد
Open برای باز کردن یک فایل ذخیره شده
Reopen: برای باز کردن فایلهایی که قبلا باز کردیم و بستیم
Save-saveas برای ذخیره فایلها بکار میرود
ftp:برای کار با ftp دانلود و اپلود فایل روی ftp بکار میرود
Encoding:برای تعیین فورمت ذخیره سازی فایل بکار میرود که به صورت پیشفرض روی ansi بوده که روی utf-8 قرار دهید
منوی Edit برای انجام کارهایی مانند cut-copy-pase-undo-redo میباشد
منوی find:برای جستجو - جانشانی و بوکمارک کردن بکار میرود
بخش جستجو دارای انتخابهایی نظیر-جستجو در سند جاری-جستجو در کلیه اسناد باز-حساسیت به حروف کوچک و بزرگ -استفاده از الگوها regular expression -استفاده از willcard نظیر * و ؟ - مارک کردن نتیجه - جستجو در فایلهای یک پوشه خاص و .... میباشد
این قابلیتها برای قسمت جانشانی replace هم صدق میکند
بوکمارک گزینه مناسبی برای وقتی که تعداد فایلها و حجم کد درون فایلها زیاد میشود میباشد .با این کار شما هر بخش از کد را که مایل باشید مارک میکنید و هر زمان که نیاز داشته باشید کافی است گزینه ان مارک را از منو انتخاب کنید تا به همان قسمت بروید

برای بوکمارک کردن کافی است تا گزینه toggle bookmarks را انتخاب و یکی از بوکمارکهای از ۰ تا ۹ را به ان اختصاص دهید و برای پرش به بوکمارک مورد نظر کافی است تا از گزینه go to bookmark بوکمارک مورد نظر را انتخاب کنید



شکل دو

منوی insert:این بخش برای اضافه کردن کدهای html به پروژه میباشد که به صورت پیشفرض تگهای انرا اماده دارد

بخش forms هم کلیه المانهای html مانند submit-input text-checkbox –radio و ... را دارا میباشد که با انتخاب یکی از انها در پنجره object inspector میتوانید خواص ان المان را کنترل کنید

منوی css:این بخش اشامل یک سری الگوها برای کد نویسی سریعتر و اسانتر css میباشد

منوی javascript : این بخش اشامل یک سری الگوها برای کد نویسی سریعتر و اسانتر جاوا اسکریپت میباشد علاوه بر این فریمورکهای معروف جاوااسکریپت مانند
Jquery – Ext js – yahoo user interface library (YUI) – Dojo –moo tools Prototype را نیز شامل میشود

منوی php: این بخش اشامل یک سری الگوها برای کد نویسی سریعتر و اسانتر پی اچ پی میباشد علاوه بر این از فریمورکهای پی اچ پی و تمپلیت انجین smarty پشتیبانی میکند و همین طور این منو دارای code beautifuler میباشد که در کد فرورفتگی و بیرون زدگی ایجاد میکند تا خوانایی کد بالاتر رود

منوی debuge:محیط توسعه پی اچ پی دیزاینر از دیباگر قدرتمند xdebuger استفاده میکند برای خطایابی و روند اجرای کدها و استفاده از قابلیتهای xcode گزینه هایی در این منو قرار داده شده است

منوی project:برای مدیریت یک پروژه نو نوشتن یک وبسایت و پوشه بندی ان از این بخش یک پروژه جدید ایجاد کرده و شروع به طراحی میکنید

منوی tools:این منو دارای ابزارهایی برای کارهای مختلف میباشد

مثلا

ftp:برای کار با ftp و اپلود و دانلود فایل یا پوشه از-به ان

Convert case:تغییر متن از حروف کوچک به بزرگ و بلعکس

Remove tag:حذف تگهای html

Thml css and javascript formatter:تنظیم فرورفتگی و برامدگی بر مبنای space مثلا هر خط 2 space

Html tidy:مقایسه html بر مبنای استاندارد مثلا استاندارد w3school

Date:تاریخ را چاپ میکند

Timestamp:تاریخ و ساعت را به چند فورمت چاپ میکند

Count:تعداد خطوط -کلامات و ... سند جاری را حساب میکند

File information:اطلاعات فایل جاری اعم از تاریخ ایجاد-تغییر و ... را نشان میدهد

Filezila وPhpmyadmin وFile diff:این بخش برای کار با این برنامه ها میباشد (این برنامه ها باید روی سیستم نصب باشند)

Export html وExport rtf وExport la tex:گرفتن خروجی از سند جاری به فورمتهای مختلف

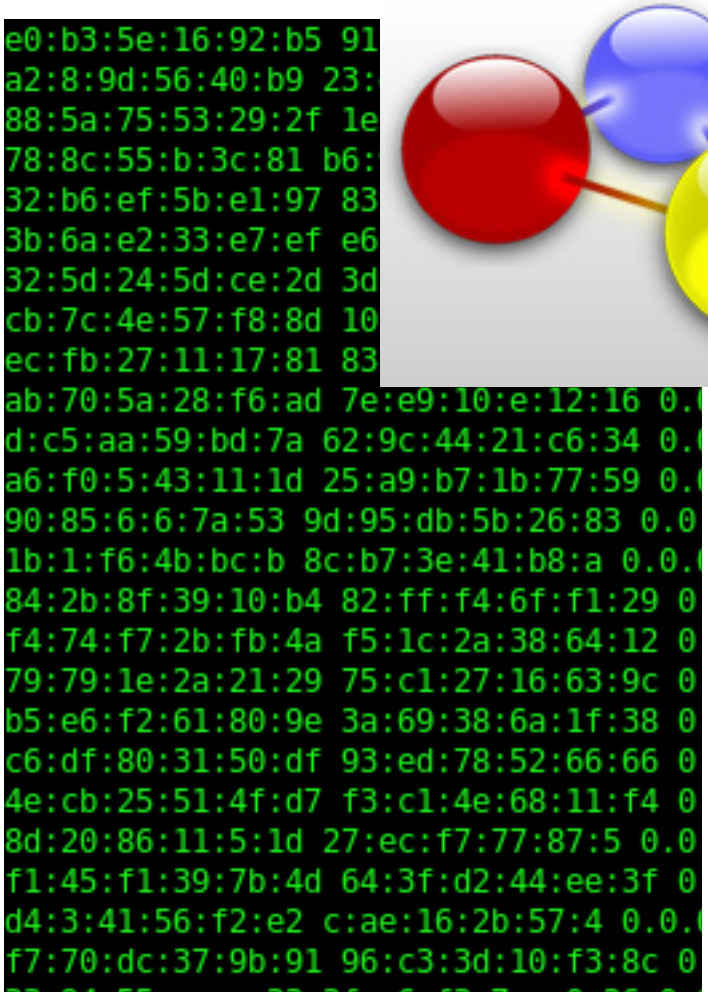
Customize:تنظیم بهتر ویرایشگر و جعبه ابزار برای دسترسی اسانتر به بخشها

منوی svn:این بخش برای کار با svn و انجام پروژه به صورت گروهی میباشد

منوی highlights:در این بخش میتوانید کلمات کلیدی هر بخش مانند perl- roby-php-css و ... از کدنویسی را مدیریت -کم یا اضافه کنید

منوی view: این قسمت برای مدیریت اجرا درون برنامه مانند ادیتور-منو-جعبه ابزار و ... استفاده کنید

منوی window:این بخش برای مدیریت پنجره ها و حالت نمایش پنجره ها میباشد



نویسنده :
AHA (godvb)

پیاده سازی حمله Mac-Flooding در مسیریاب سیسکو

مقدمه :

در این مقاله مبحث ما،آموزش سیسکو کانفیگ روترها و ... نیست. در این مقاله سعی براین است که بتوانیم پیرو مقاله قبلی («چگونه یک آزمایشگاه تست نفوذ داشته باشیم») بحث را کمی پیشرفته ترکنیم. در مقاله قراراست یک شبکه را پیاده سازی کنیم، مانند روتر و سوییچ ها و توسط سیستم عامل بک ترک یک از متدهای نفوذ را اجرا نماییم.

در این شبکه ما قصد پیاده سازی حمله از نوع Mac-Flooding را داریم.

GNS3 چیست؟

GNS3 یک شبیه ساز گرافیکي شبکه میباشد که به کمک آن میتوان شبکه هاي پیچیده را شبیه سازي نمود. این نرم افزارمیتواند در طرحهاي آزمایشي IOS Cisco یا به منظور بررسي کردن پیکربندي که براي یك شبکه نیاز است مورد استفاده قرار بگیرد. برنامه رایگاني است که امکان استفاده از آن روي چندین سیستم عامل مانند ویندوز ، لینوکس و MAC OS وجود دارد. از IOS هاي تجهیزات مختلفي از جمله روتر، Frame ، ATM Relay ، سوئیچهاي لایه دو و همچنین PIX firewalls پشتیباني مینماید.این نرم افزار شبیه ساز را میتوان از لینک زیر دانلود نمود :

http://www.gns3.net/download/

حملات MAC Address Flooding

جدا از طرز کار Hub ها که هیچ هوشمندی ندارند، سوییچ ها در لایه ۲ از مدل OSI دارای مرحله ای به نام Learning هستند، بدین معنا که هر فریمی را که دریافت می کنند بخش Source MAC از فریم را میخواند و متوجه می شود که برروی پورت دریافتی دستگاهی با چه MAC Address قرار دارد و همچنین مربوط به کدام VLAN است

سپس آن را در جدولی که به نام Cam Table[1] درج میکند. هنگامی که CAM Table تکمیل شد، سوییچ براحتی میتواند بسته های دریافتی را به خروجی مناسب هدایت کند. جهت فهمیدن مرحله Learning و حمله MAC Address Flooding در ادامه با تصاویر توضیح داده خواهند شد.

با اجرا دستور زیر در سوییچ می توانید جدول را ببینید : (شکل یک)

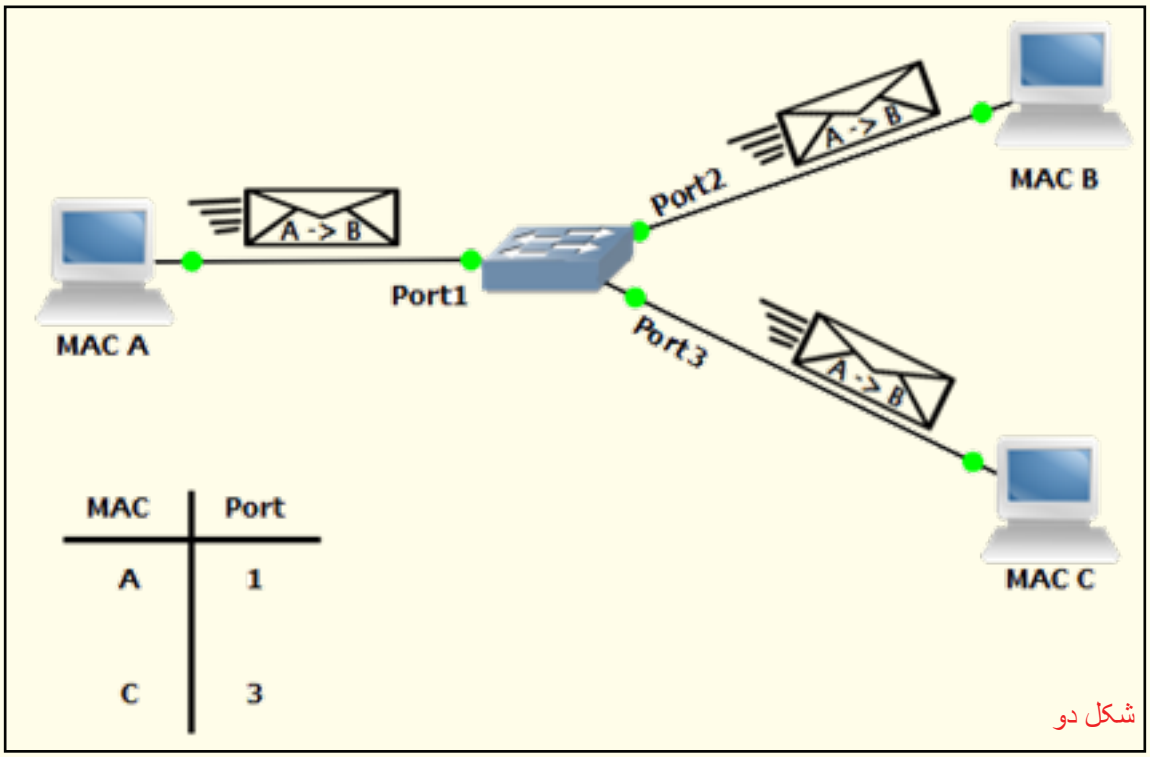
show mac-address-table

```
DSW1#show mac-address-table
        Mac Address Table
-------------------------------------------

Vlan   Mac Address      Type        Ports
----   -----------      --------    -----
All    0014.6922.5440   STATIC      CPU
All    0100.0ccc.cccc   STATIC      CPU
All    0100.0ccc.cccd   STATIC      CPU
All    0100.0cdd.dddd   STATIC      CPU
1      0f08.0a01.9b54   DYNAMIC     Fa0/1
1      0f08.0a02.42f9   DYNAMIC     Fa0/2

Total Mac Addresses for this criterion: 26
```

شکل یک

۱ Addressable Memory Content

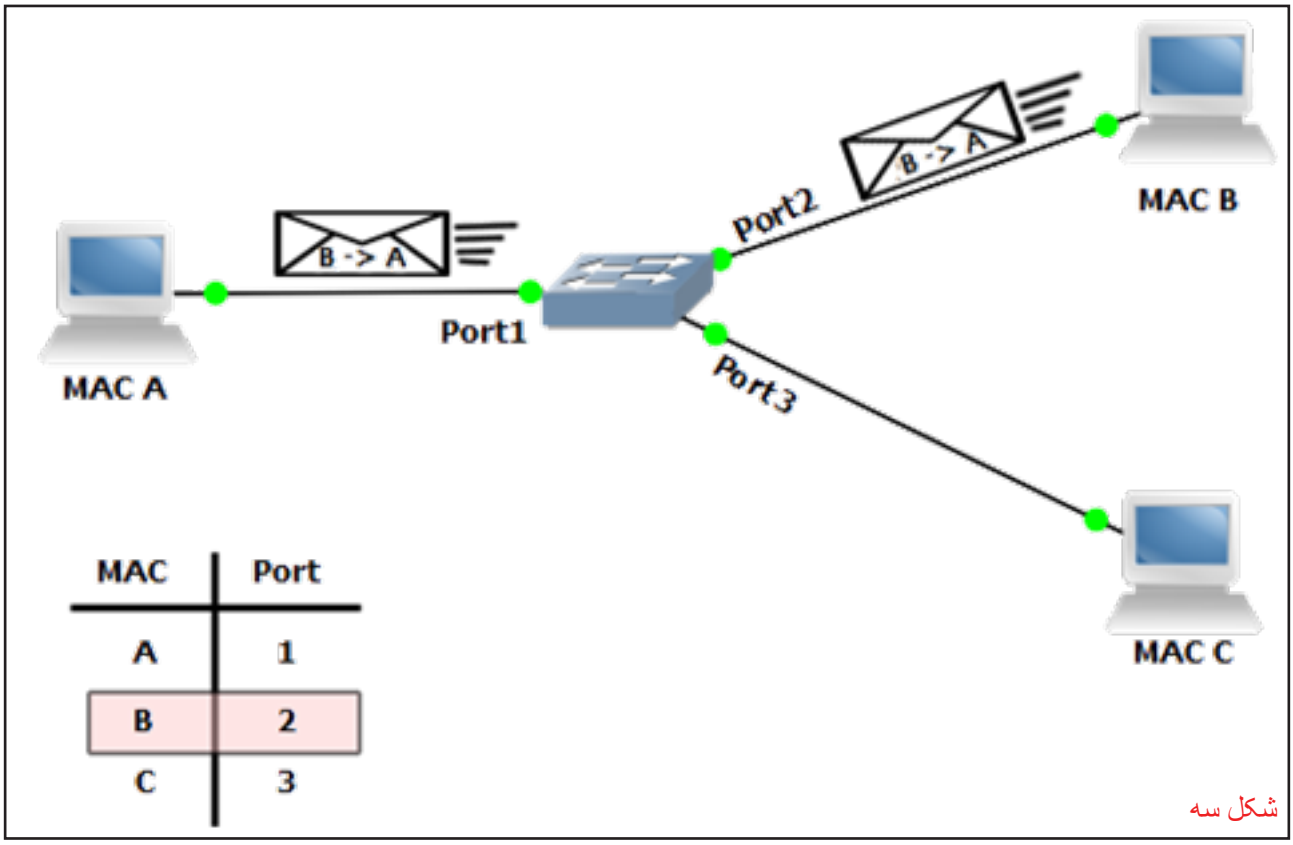
اگر سوییچ فریمی را دریافت کند و MAC Address آن در جدول وجود نداشته باشد، سوییچ مانند Hub عمل میکند و فریم دریافت شده را برروی تمامی پورت های خود ارسال میکند. در شکل دو بهتر متوجه این عمل خواهید شد



شکل دو

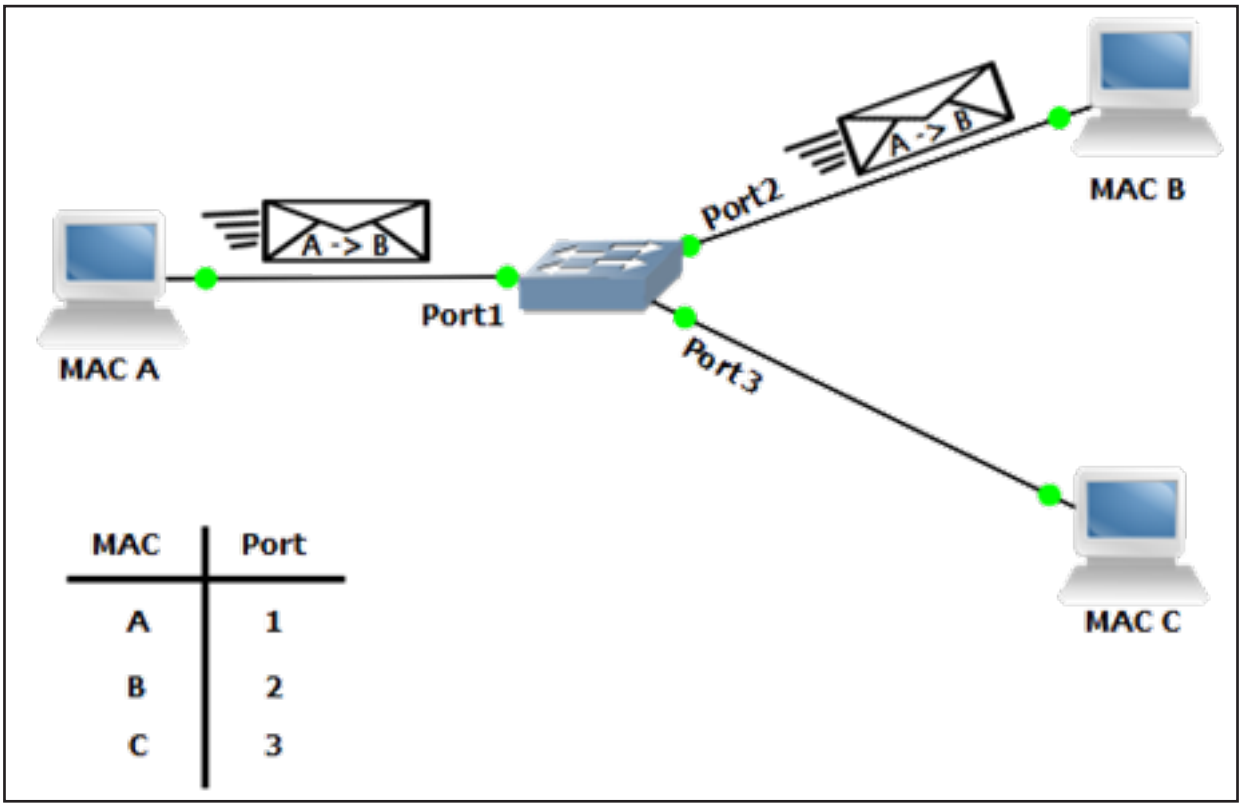
سیستم A میخواهد داده ای را برای سیستم B بفرستد ولی پورتی برای آن در جدول تعریف نشده است پس فریم دریافتی را Broadcast میکند. فریم برای سیستم c هم ارسال می شود، ولی چون Des MAC (آدرس mac مقصد) با سیستم c یکسان نیست متوجه خواهد شد که فریم دریافتی متعلق به او نیست بنابراین فریم را از بین خواهد برد.

در تصویر زیر (شکل سه) میبینید که بسته ای از سیستم B دریافت شده است، ابتدا Source MAC را میخواند در جدول وجود ندارد پس آن را درج می کند. سپس Des Mac را میخواند که مربوط به سیستم A می باشد و رکوردی برای آن در جدول وجود دارد بنابراین فریم را به خروجی مناسب هدایت میکند. حال که رکوردی برای سیستم B در جدول وجود دارد پس دیگر عمل Broadcast انجام نخواهد شد:



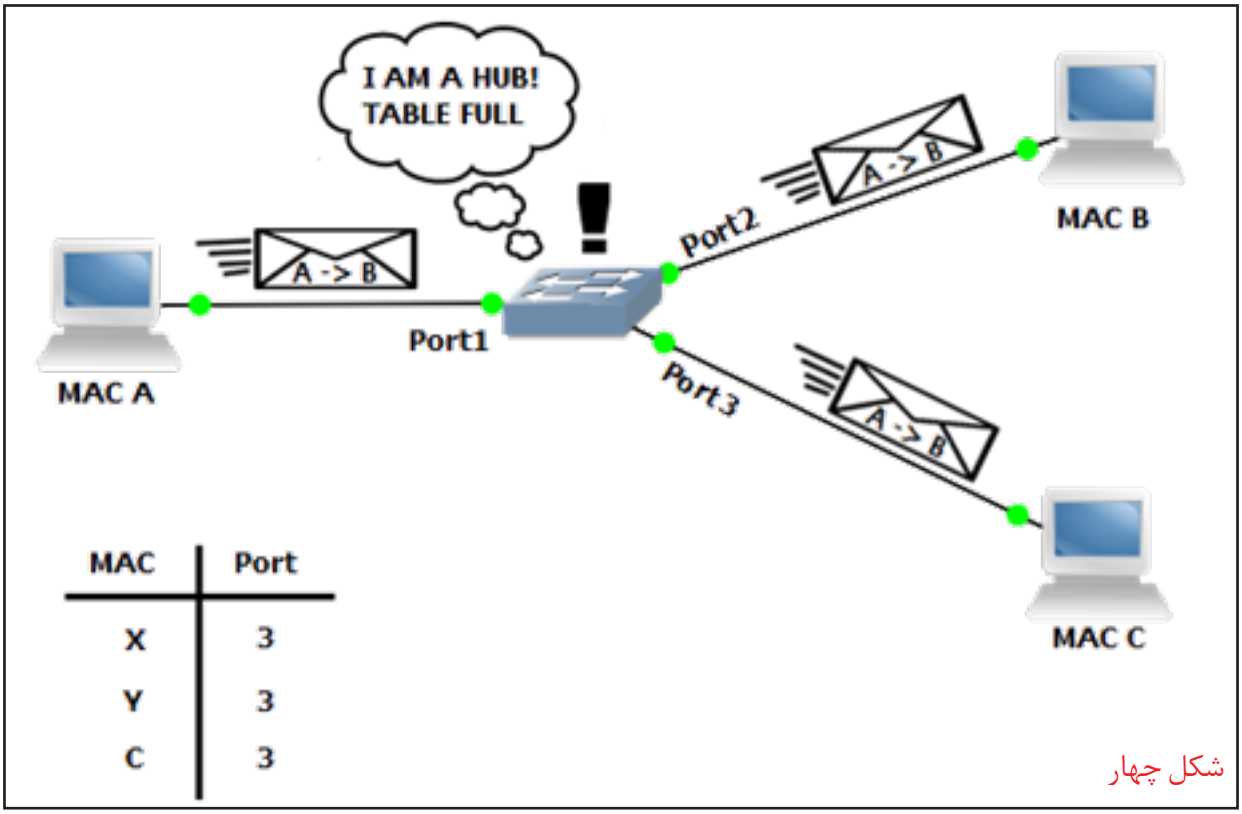
شکل سه

در حالت نرمال پس از گذر از مراحل قبل (Learning) جدول کامل شده است. اگر اطلاعاتی را برای سیستمی خاص، در یک شبکه بخواهیم ارسال کنیم از آنجایی که در لایه دو هستیم و با فریم ها سروکار داریم، سوییچ مان تنها MAC Address را می شناسد، بعد از دریافت فریم و خواندن بخش Des MAC و جستجوی آن در جدول پورت خروجی مناسب را برای هدایت فریم انتخاب میکند. این روند کار باعث شد تا سوییچ دارای Collision Domain Per Port شود.



حال اگر یک هکر قصد داشته باشد به شبکه مان حمله کند چه اتفاقاتی خواهد افتاد؟ حمله کننده (Attacker) می داند که حافظه برای ذخیره اطلاعات جدول محدود است، پس با ارسال فریم با Source MAC های جعلی سعی بر پر کردن این جدول میکند(در سوئیچ ۳۷۵۰ در حدود ۶۰۰۰ جاي خالي وجود دارد).

هنگامی که جدول سرریز شود دیگر سوییچ مانند هاب عمل کرده و تمامی فریم ها را Broadcast می کند(شکل چهار). Attacker چگونه این عمل را انجام میدهد ؟ توسط ابزارهایی که در ادامه یک نمونه آن معرفی می شود سعی بر ایجاد SOurce MAC های جعلی و ارسال سیل آسا آن به سمت سوییچ می کند. زمانی که جدول MAC Address هایمان پر شود و تمامی پورت های آن توسط ترافیک ورودی مشغول شد دیگر آدرس را نمی تواند در جدول خود براحتی پیداکند و مانند هاب عمل خواهد کرد. ابزارهای برای حمله تقریبا ۱۶۰,۰۰۰ فریم در دقیقه می توانند ایجاد کنند و برای سوییچ ارسال کنند که شامل Source,Destination MAC و IP Address بصورت رندوم می باشد



شکل چهار

ابزارهای مختلفی برای حملات لایه ۲ موجود است مانند : Yersinia , EtterCap و ....

یکی از ابزارهایی که می توان این عمل را انجام دهیم macof است که میتواند در دقیقه ۱۵۵,۰۰۰ آدرس ایجاد کند. بصورت زیر می توان آن را استفاده نماییم :

```
macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]
```

اگر در هربخش مقدارهایی را ست نکنیم، بصورت random در برنامه مقدار دهی خواهند شد. براحتی توسط دستورات زیر می توان آن را در Backtrack اجرا نماییم و با زدن CTRL+Z حمله را متوقف کنیم.

```
root@bt:~/# macof
root@bt:~/# ^Z
```

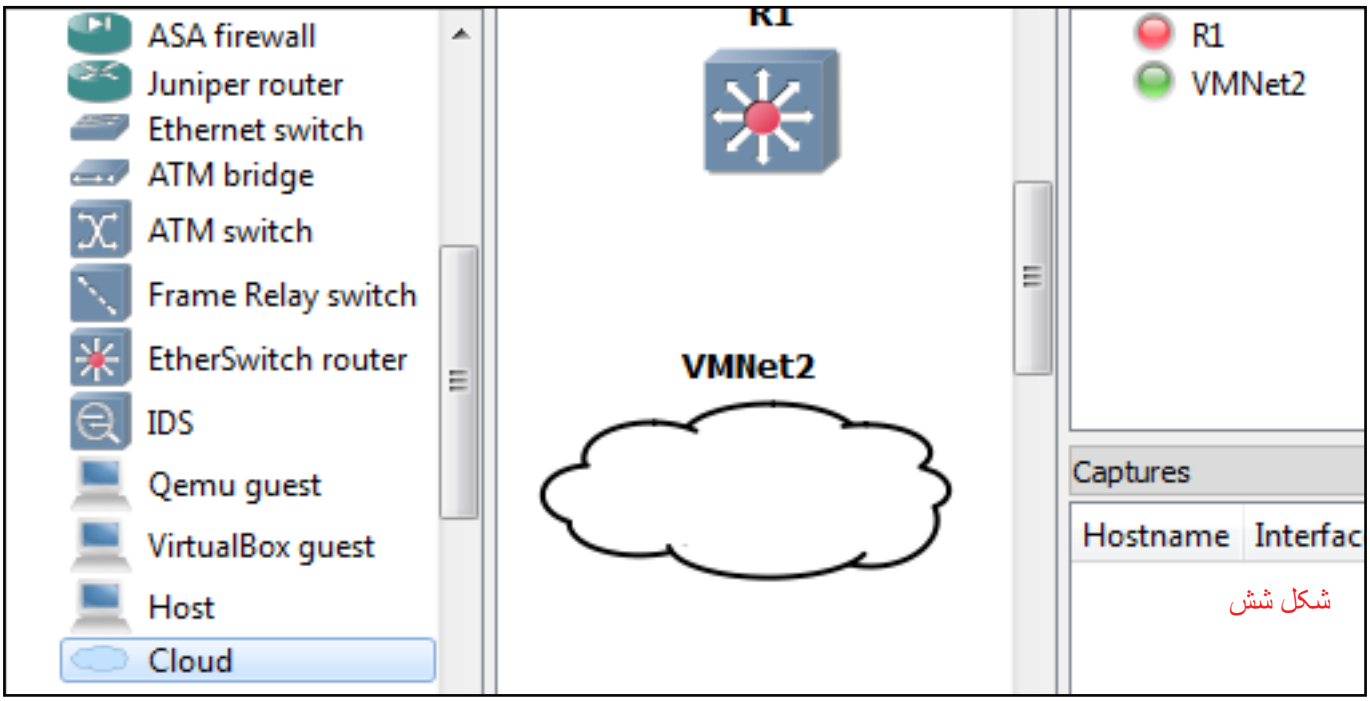
حال با اجرای یک اسنیفر راحت فریم ها را می توانید دریافت کنید

پس از آشنایی با ساختار این نوع حمله ابتدایی؛ حال به سراغ کار عملی میرویم.

ابتدا یک ماشین مجازی داریم که در آن بک ترک را نصب کرده ایم (من Backtrack5 r2 را نصب کرده ام). اینترفیس شبکه آن را برروی vmnet2 تنظیم میکنیم(در setting ماشین مجازی ساخته شده و بخش network adapter). در Virtual Network Editor نگاه کنیم میبینیم که vmnet2 دارای چه رنج از IP است و در بک ترک اینترفیس مان را براساس آن IP می دهیم، به ترتیب از مرحله یک تا چهار (شکل پنج).

برای آشنایی با ماشین مجازی به شماره دوم مجله ایرانویج (آبان ۹۱) مراجعه کنید.

بعد از انجام این کار بایستی عملیات را در GNS3 هم انجام دهیم،GNS3 را بازکرده و متناسب با تصویر زیر یک Cloud و یک Ethernet Switch قرار می دهیم (شکل شش)؛ سپس برروی Cloud دوبارکلیک کرده تا پنجره شکل هفت بازشود و در آن اینترفیس مجازی vmnet2 در سیستم مان را به آن اضافه می کنیم،درقسمت Generic Ethernet NIO اینترفیس را انتخاب کرده و Add را میزنیم (شکل هفت).



شکل شش

Node configurator

Clouds
VMNet2

VMNet2 node

NIO Ethernet | NIO UDP | NIO TAP | NIO UNIX | NIO VDE | NIO NULL

Generic Ethernet NIO (Administrator or root access required)

rpcap://\Device\NPF_{5508D08F-A63C-41B5-90E0-22B7D262669F} : Network

' on local host: VMware Network Adapter VMnet2 | Add | Delete

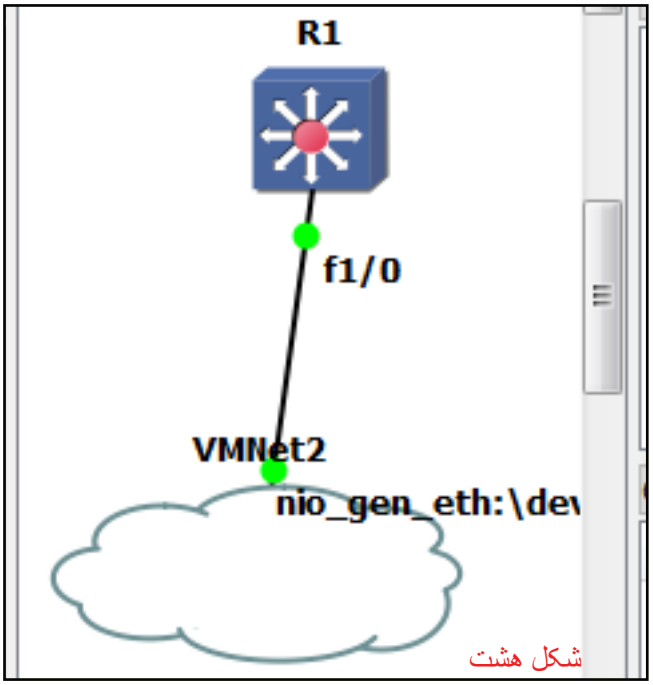
nio_gen_eth:\device\npf_{5508d08f-a63c-41b5-90e0-22b7d262669f}

Linux Ethernet NIO (Linux only, root access required)

Add | Delete

شکل هفت

Reset | OK | Cancel | App



شکل هشت

سپس Cloud را توسط یک ارتباط Fast Ethernet به اینترفیس شماره ۰/۱ از Ethernet switch وصل می کنیم(در تولبار برروی شکل سوکت کلیک کنید). از منوی Control -> Start/resume all device را میزنیم. خوب تا به اینجا باید شکلی بدین صورت داشته باشیم (شکل هشت)

حال برروی Ethernet Switch دابل کلیک کرده و دستورات زیر را وارد می کنیم(بعداز دابل کلیک برنامه Putty بصورت پیش فرض اجرا خواهد شد):

```
R1#conf t
R1(config)#int f 1/0
R1(config-if)#sw mod acc
R1(config-if)#sw acc vlan 1
R1(config-if)#ex
R1(config)#int vlan 1
R1(config-if)#ip add 192.168.234.10 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ex
```

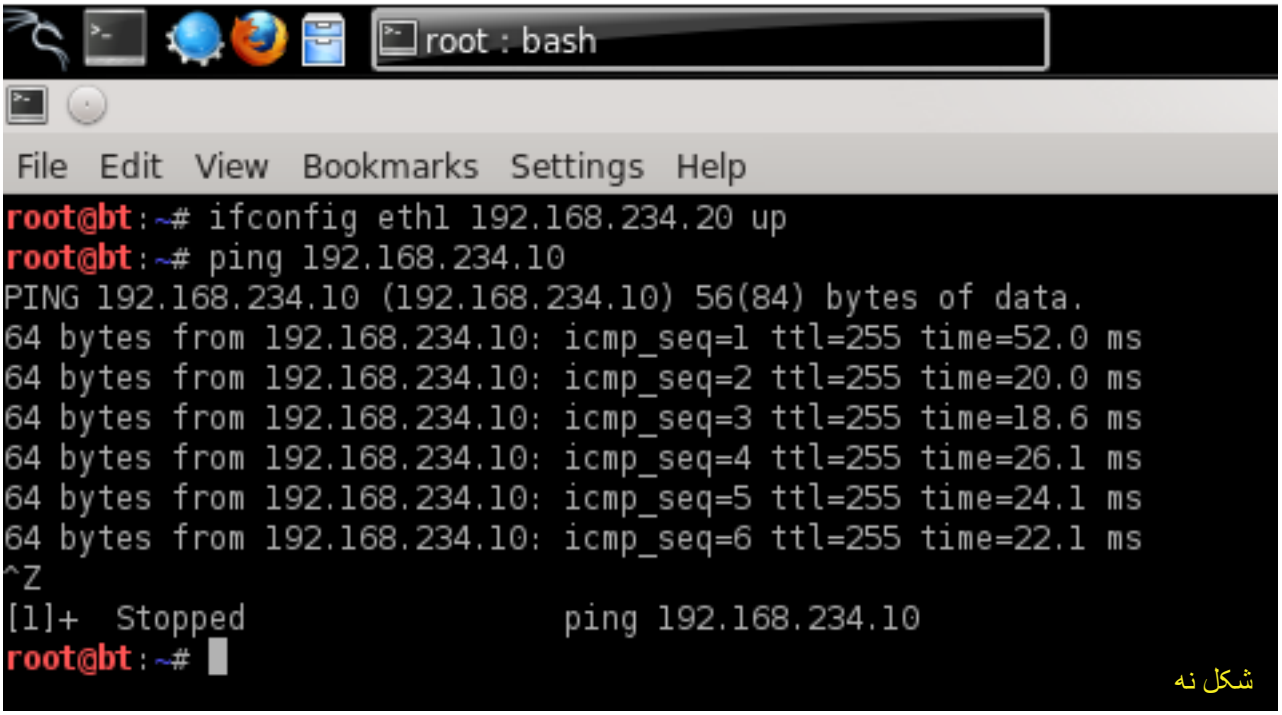
دردستورات بالا به اینترفیس از سوییچ IP که ست نموده ایم ۱۹۲.۱۶۸.۲۳۴.۱۰ است که در همان رنج از IP که در بک ترک ست نمودیم.

تا به اینجا کار ما تمام شد و ارتباط بین سیستم عاملمان (بک ترک) و سوییچ برقرار است، می توانیم Ping نماییم تا ببینیم ارتباط برقرار است یا نه (شکل نه).

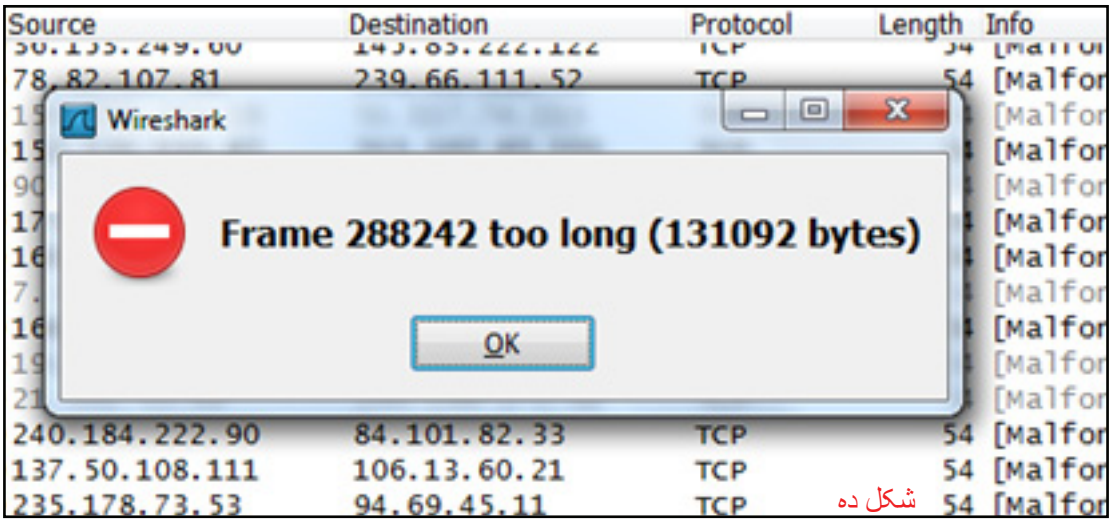
حال اگر در سوییچ دستور زیر را اجرا نماییم متوجه میشویم که تنها یک آدرس MAC را Learn نموده است :

```
R1(config)#do sho mac-add
Destination Address  Address Type  VLAN  Destination Port
------------------- ------------ ---- --------------------
c400.0908.0000       Self        1    Vlan1
```

حالا آخرین مرحله حمله را آغاز می کنیم تا CAM Table سوییچ را پودر کنیم!!! در بک ترک macof را اجرا میکنیم و دوباره cam table را نگاه میکنیم تا متوجه شویم چند آدرس MAC را Learn نموده است ، اگر در حین حمله Wireshark را اجرا کنید بعد از چندین ثانیه پیغام خطایی مانند زیر را مشاهده می کنید(شکل ده).



شکل نه



شکل ده

حال CAM Table را مشاهده میکنیم :

```
R1(config)#do sho mac-add
Destination Address  Address Type  VLAN  Destination Port
------------------- ------------ ---- --------------------
c400.0908.0000       Self        1    Vlan1
000c.299d.7832       Dynamic     1    FastEthernet1/0
e835.0a5b.60c3       Dynamic     1    FastEthernet1/0
6215.dd4b.911a       Dynamic     1    FastEthernet1/0
be66.8e54.7497       Dynamic     1    FastEthernet1/0
624d.3f75.81c6       Dynamic     1    FastEthernet1/0
08aa.325a.e277       Dynamic     1    FastEthernet1/0
8276.ae4c.e108       Dynamic     1    FastEthernet1/0
94b0.7955.53ae       Dynamic     1    FastEthernet1/0
b0f8.9a3e.02db       Dynamic     1    FastEthernet1/0
22d3.5051.4c52       Dynamic     1    FastEthernet1/0
1472.c950.ef88       Dynamic     1    FastEthernet1/0
16db.a35a.c3e8       Dynamic     1    FastEthernet1/0
465d.0547.bad7       Dynamic     1    FastEthernet1/0
1015.9025.db99       Dynamic     1    FastEthernet1/0
9af1.9b3a.e525       Dynamic     1    FastEthernet1/0
76de.880a.495a       Dynamic     1    FastEthernet1/0
aea1.052b.6f9a       Dynamic     1    FastEthernet1/0
8648.366a.fa9a       Dynamic     1    FastEthernet1/0
3ad5.aa12.1963       Dynamic     1    FastEthernet1/0
7a2f.b43b.4cdd       Dynamic     1    FastEthernet1/0
 --More—
```

نکات قابل ذکر در این نوع حمله :

۱ - اگر هرلحظه تعداد آدرس های CAM Table را بگیرید میبینید که :

```
R1#sho mac-ad count
NM Slot: 1
--------------
Dynamic Address Count:                 8188
Secure Address (User-defined) Count:   0
Static Address (User-defined) Count:   0
System Self Address Count:             1
Total MAC addresses:                   8189
Maximum MAC addresses:                 8192
R1#
```

میبینید که مقدار Total و maximum یکسان نیست .

۲ - اگر macof را کنسل کنید و دوباره دستور قبل را اجرا کنید میبینید که :

```
R1#sho mac-ad count
NM Slot: 1
--------------
Dynamic Address Count:                 0
Secure Address (User-defined) Count:   0
Static Address (User-defined) Count:   0
System Self Address Count:             1
Total MAC addresses:                   1
Maximum MAC addresses:                 8192
R1#
```

همه چیز به حالت طبیعی برگشت .

این یکی از ساده ترین و پیش پاافتاده ترین نوع حمله از حملات لایه ۲ است که انجام دادیم ، هدف در این مقاله آشنایی با تست نفوذ و نحوه کار بوده است نه حمله واقعی ، پس خوشحال باشید که حالا می توانید حملات دیگر را پیاده سازی کنید .

فایل های مورد نیاز و تنظیمات سویچ ارایه شده در این مقاله در فایلهای پیوست شده به مجله به نام MAC-FLOODING موجود است

سری آموزش های پایتون

قسمت اول

آموزش Eclipse

نویسنده:
AHA(godvb)

Eclipse چیست؟

می توان گفت یک IDE که تحت لیسانس GPL و سورس باز میباشد. این محیط توسعه روند جدید رو در پیش گرفته، وقتی این محیط را بصورت معمولی و عادی دانلود کنید امکانات بسیاری در اختیارتان قرار نمیدهد و حتی روند برنامه نویسی ویژوال (مثل طراحی فرم و ...) را ندارد و حتی برنامه نویسی تحت وب و خیلی از گزینه ها رو پشتیبانی نمیکند.

اما در عوض این سیستم طی روند جدیدی به افراد اجازه میدهد تا اجزا وافزودنی های خاص خودش (Plug-In) را نوشته و از آن استفاده کنند. اما خبر بهتر آنکه گروه توسعه دهنگان این IDE پلاگین های مورد نیاز را هم به صورت جدا نوشتند و برای دانلود رایگان در ااینترنت گذاشته اند. مثلا برای طراحی و توسعه محیط تحت وب در اکلیپس یک پلاگین پر طرفدار بنام WebTools وجود دارد که تمامی نیازهای برنامه نویسی تحت وب از دیتا بیس تا طراحی css ها رو پشتیبانی میکند. همچنین پلاگین های زیادی برای ابزار مدلینگ و یا طراحی گرافیکی و .... طراحی شده است.

اما شاید برای افراد جالب باشه که این محیط فقط و فقط برای زبان برنامه نویسی جاوا نیست و پلاگین هایی برای زبان های برنامه نویسی C/C++ , php , COBOL , Fortran را نیز دارد .

برای دانلود این IDE می توان به آدرس زیر رفته و نسخه مناسب با سیستم عامل خود دانلود نمایید:

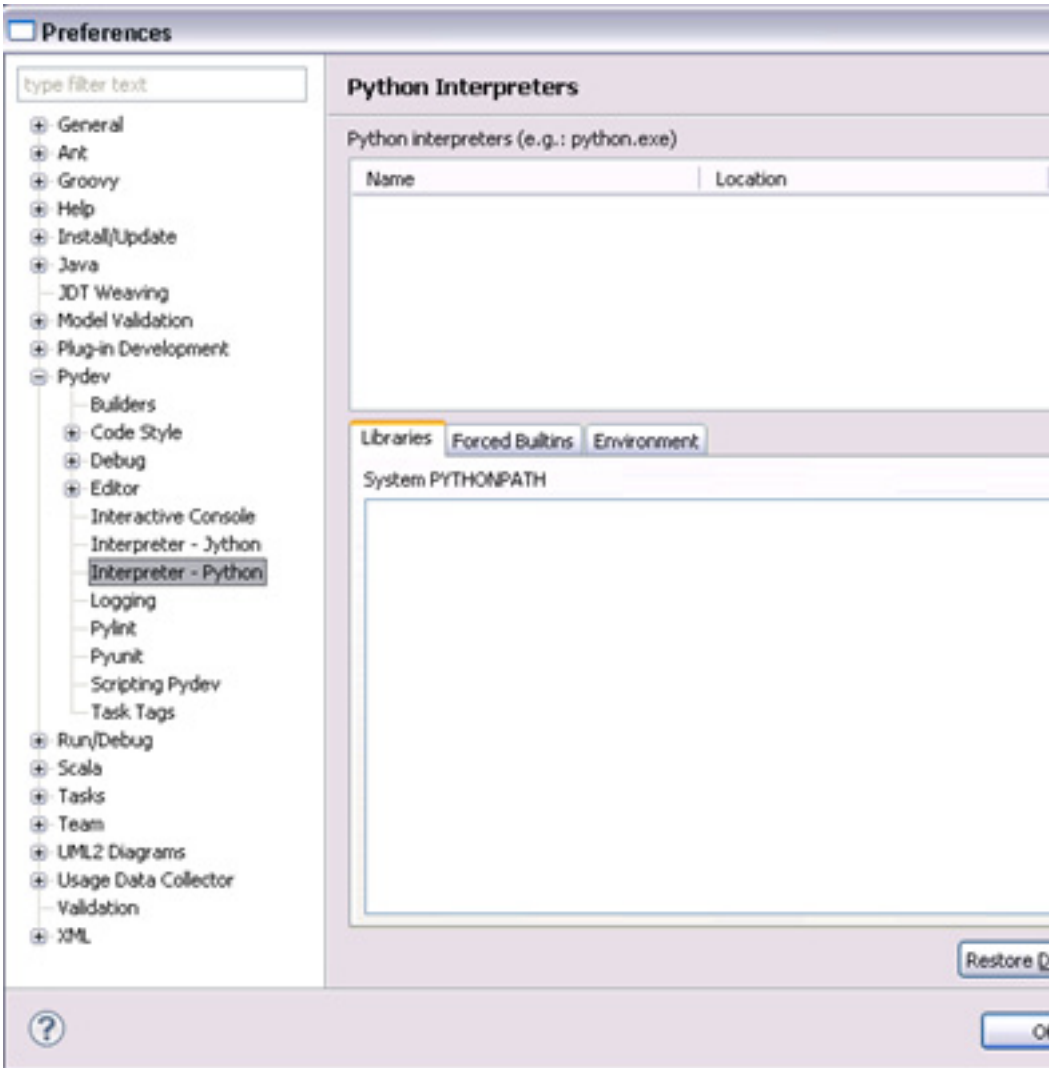
http://www.eclipse.org/downloads

نسخه های مختلفی از این IDE برای دانلود قرار دارد، برای پایتون می توان Eclipse Classic را دانلود نمایید.

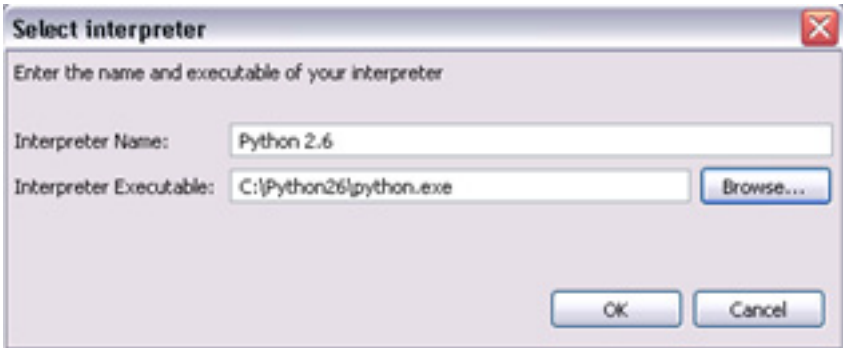
پلاگین pydev

با کمک این افزونه plugin میتوان امکان برنامه نویسي براي پایتون را به eclipse اضافه کرد. این پلاگین را نیز می توانید از لینک زیر دریافت نمایید:
http://pydev.org/download.html

پلاگین PyDev بصورت روبرو است و دارای دو پوشه میباشد که بایستی در مسیر نصب eclipse/dropins آن را paste نمایید، در هنگام انجام این عمل اگر پیغامی مبنی بر موجود بودن فایل ها مشاهده نمودید، Replace نمایید

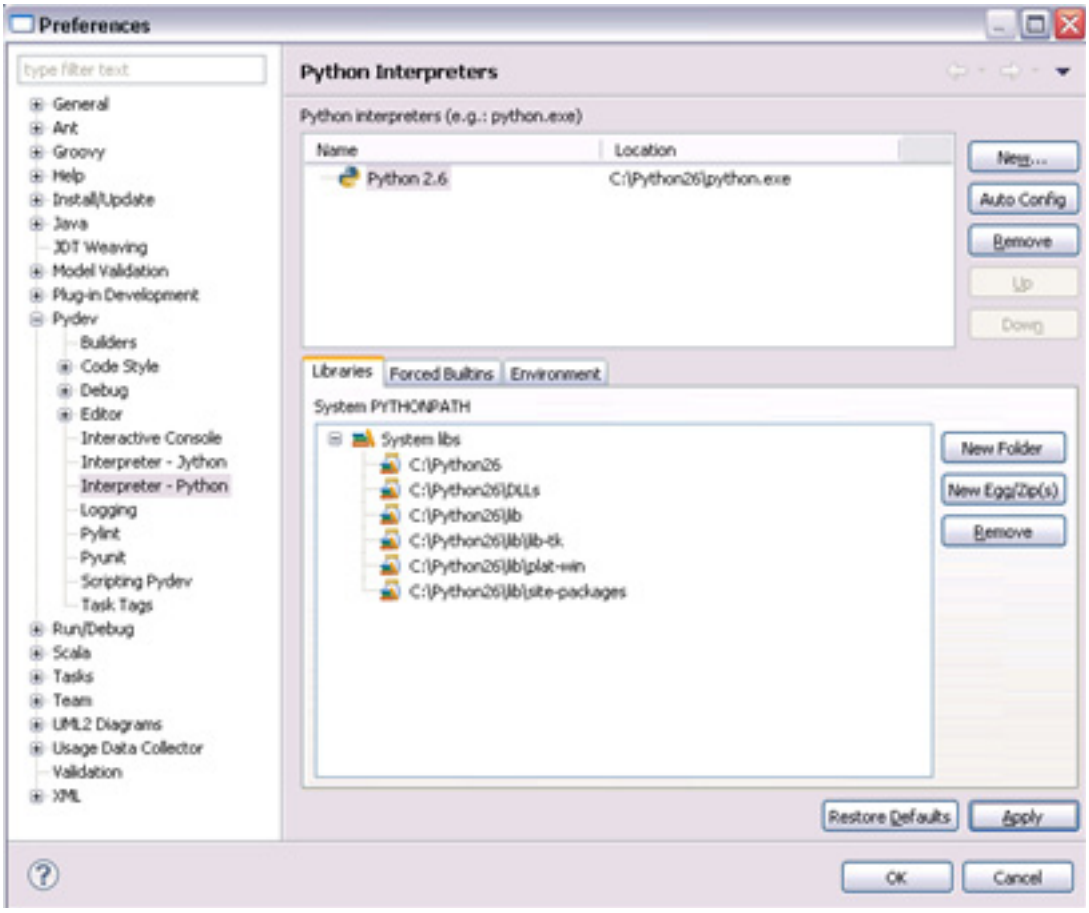


بعد از نصب eclipse و pydev به منوی
Window -> Preference
رفته و از ساختار درختی سمت چپ
Pydev-> Interpreter Python
را انتخاب کنید



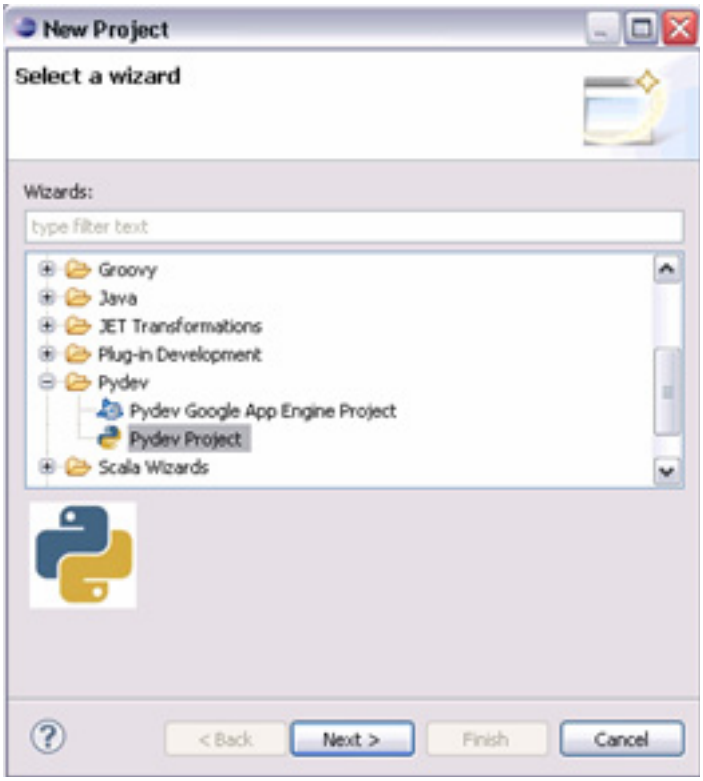
سپس بعد از کلیک برروی دکمه new بایستی به مسیر نصب پایتون رفته و فایل python.exe را انتخاب نمایید

که در پایان بایستی نتیجه ای بدین صورت داشته باشید



حال هرنسخه از پایتون راکه در سیستم خود نصب کرده اید را می توانید به لیست اضافه نمایید به این دلیل که در هنگام ساخت پروژه تعیین میکنید مفسر کدام نسخه از پایتون برای پروژه تان اعمال گردد.

اولین برنامه



به منوی

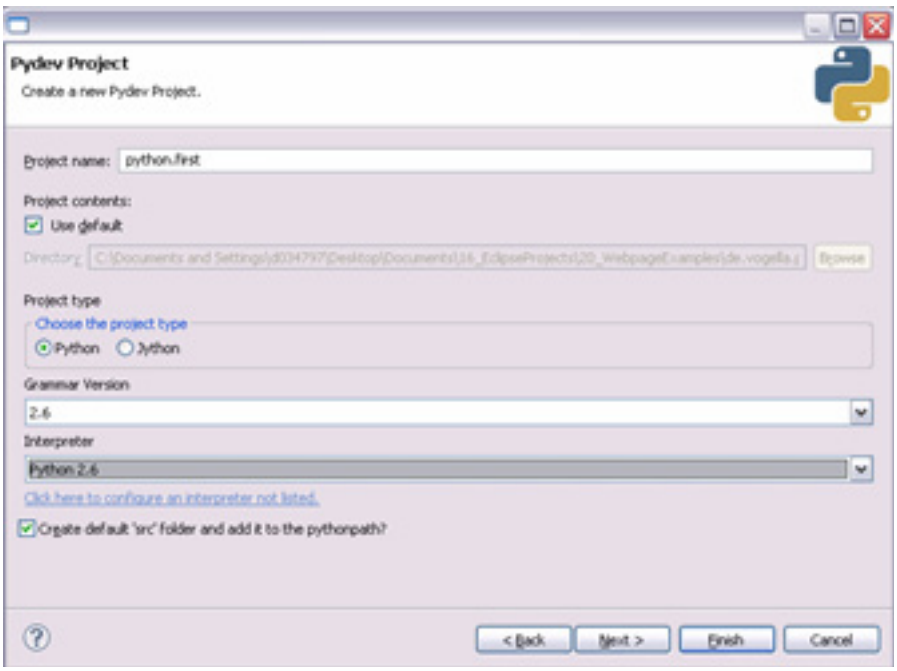
File -> New -> Project

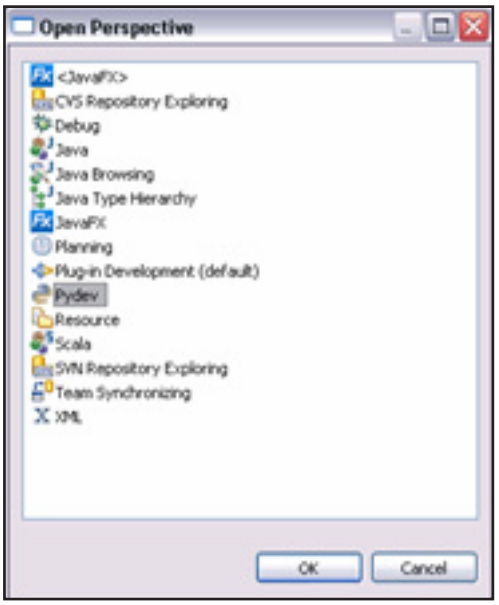
رفته و در پنجره ایجاد شده (شکل زیر) گزینه

Pydev -> Pydev Project

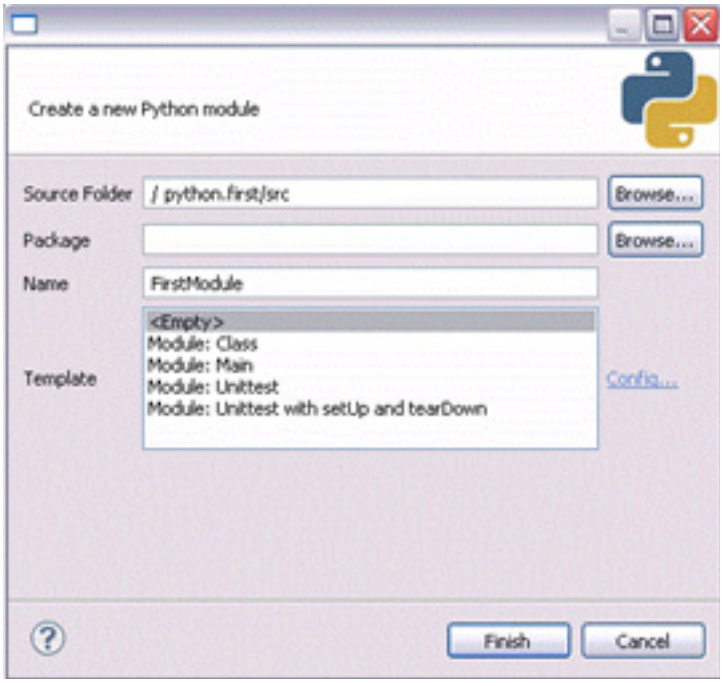
را انتخاب نمایید:

سپس نام پروژه جدید را python.first و مفسر را نسخه ۲.۶ از پایتون انتخاب میکنیم

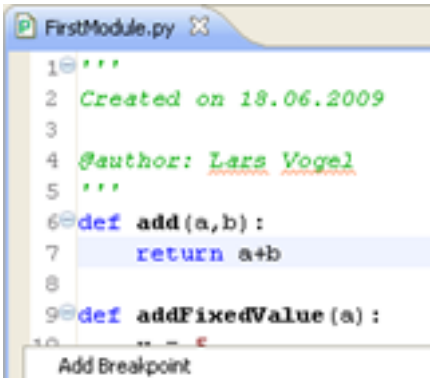




برای نمایش و ظاهر (Perspective) در eclipse از منوی
Window->Open Perspective ->Other
رفته و حالت PyDev را انتخاب میکنیم



سپس برروی پوشه «src» کلیک راست نموده و گزینه
New -> PyDev Modul
را انتخاب می کنیم تا اولین ماژول را برای کد نویسی ایجاد نماییم



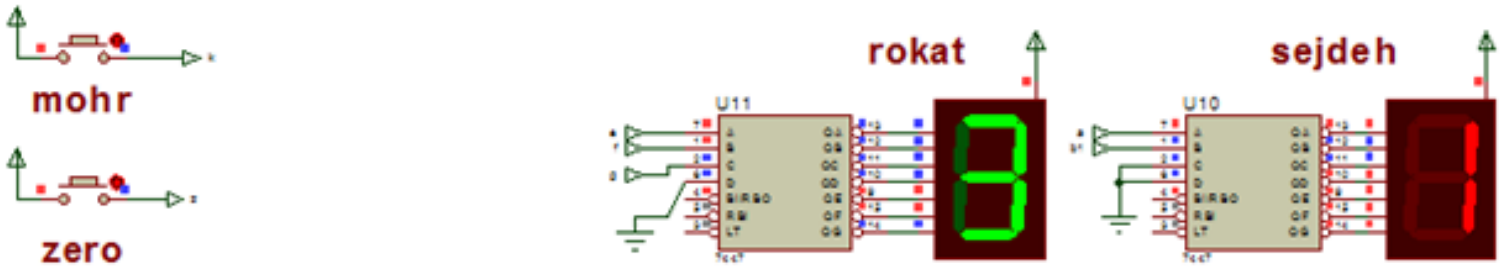
سپس کدهای مورنظرتان را درون ماژول ایجاد شده بنویسید. برای اجرای کدهای نوشته شده، برروی ماژول کلیک راست نموده و Run as -> Python Run را انتخاب کنید، تبریک میگم شما اولین برنامه در پایتون را نوشتید و اجرا نمودید. میتوانید خروجی هایتان را دربخش کنسول که معمولا بخش زیرین سورس کدهایتان قرار دارد ببینید.
برای حالت دیباگ هم میتوانید برروی سورس کدهایتان کلیک راست نمایید و گزینه Add Breakpoint را بزنید
دقت کنید برروی ستون خاکستری رنگ که در کنار اعداد است بایستی کلیک راست نمایید.
برای اجرا بصورت دیباگ برروی فایل راست کلیک کرده و Debug as -> Python Run را انتخاب کنید، میتوانید مراحل دیباگ و اجرا را از منوی RUN هم انجام دهید

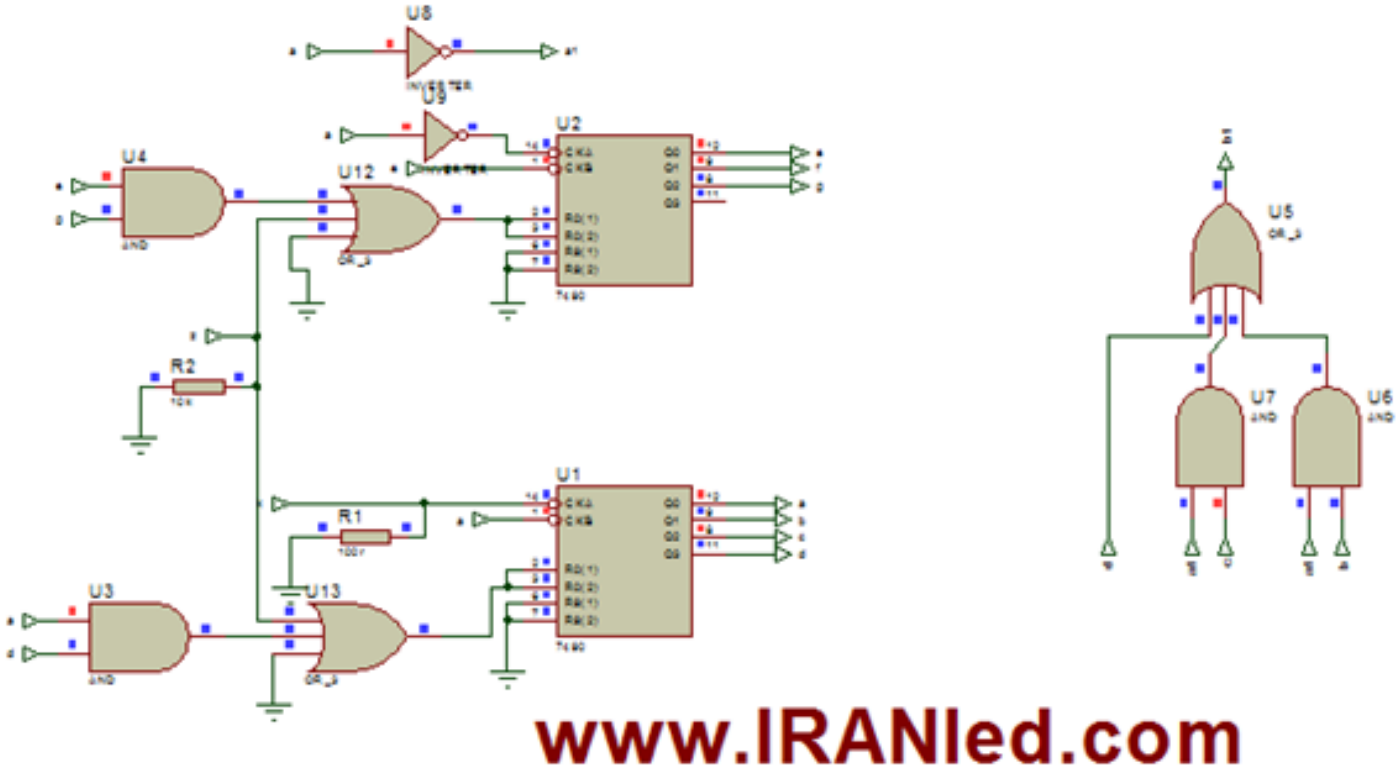
و همچنین میتوان با دکمه های موجود بصورت UI این اعمال را انجام داد

پروژه الکترونیکی مهر امین

نویسنده:
hadikh73

پروژه ای که برای این شماره در نظر گرفته شده؛ مهر امین نام دارد که با استفاده از مدار منطقی ساخته شده است و دارای قابلیت شمارش رکعت و سجده را به صورت مجزا و همچنین قابلیت صفر شدن را دارد
این پروژه از آی سی های ۷۴۴۷ و ۷۴۹۰ و...





فایهای مورد نیاز در پوشه mehramin موجود است

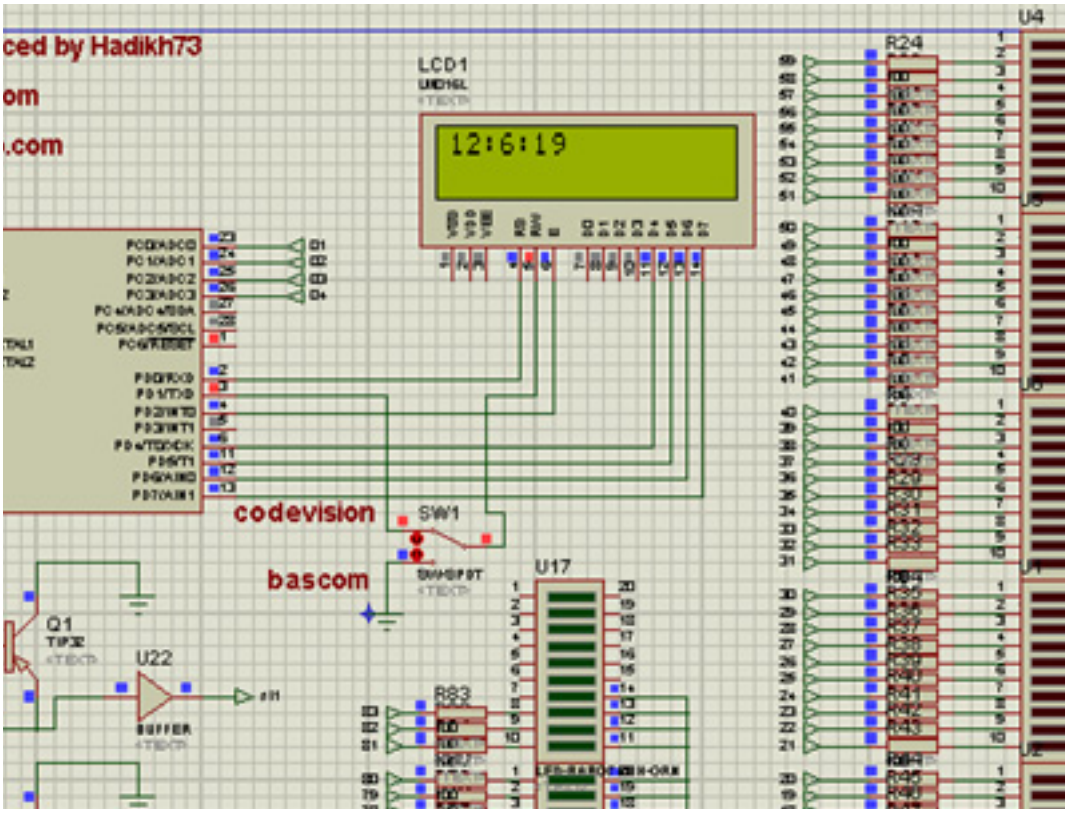
ساعت led

نویسنده:
hadikh73

در این قسمت یک پروژه ساعت LED داریم که به ازای اضافه شدن هر دقیقه یک ال ای دی بیشتر روشن می شود . این ساعت از یک atmega8 و یک ال سی دی کاراکتری(فقط جهت تست مدار آورده شده است و می توانید آن را حذف کنید) و ۱۱ عدد آی سی ۷۴۱۶۴ و ... ساخته شده است

روش تنظیم:

۱. با فشار دادن کلید namayesh ساعت نمایش داده می شود
۲. برای تنظیم ساعت باید زمانی که ال ای دی ها روشن هستند با کلید saniye=0 ثانیه شمار را صفر کنید با کلید های saat++ و daghighe++ به ترتیب یک دقیقه و یک ساعت اضافه کنیم



پروژه کامل به همراه فایهای مورد نیاز در پوشه led موجود است

طریقه اندازه گیری دمای منفی با LM35

نویسنده: r0b0

مشکل جمع کثیری از افراد اندازه گیری دمای منفی با سنسور LM35 هست که در این پروژه قصد داریم حداکثر بازه دما رو با این سنسور اندازه گیری کنیم ، یعنی دمای 55- درجه تا 155+ درجه.

برای این منظور ابتدا مدار زیر را می بندیم

که قطعات مورد نیاز این پروژه به شرح زیر است

۱. میکرو avr
۲. سنسور lm35
۳. مقاومت 10k
۴. دیود 1n4148
5. lcd 2*16
۶. و یک شارژر 5 ولتی

برنامه پروژه به زبان بیسیک نوشته شده است که در ضمیمه همزاه مجله موجود است

توضیح برنامه

در این برنامه بعد از معرفی میکرو و فرکانس و پیکر بندی پورت ها، lcd سنسور را پیکر بندی می کنیم و بعد اصل برنامه نوشته می شود؛

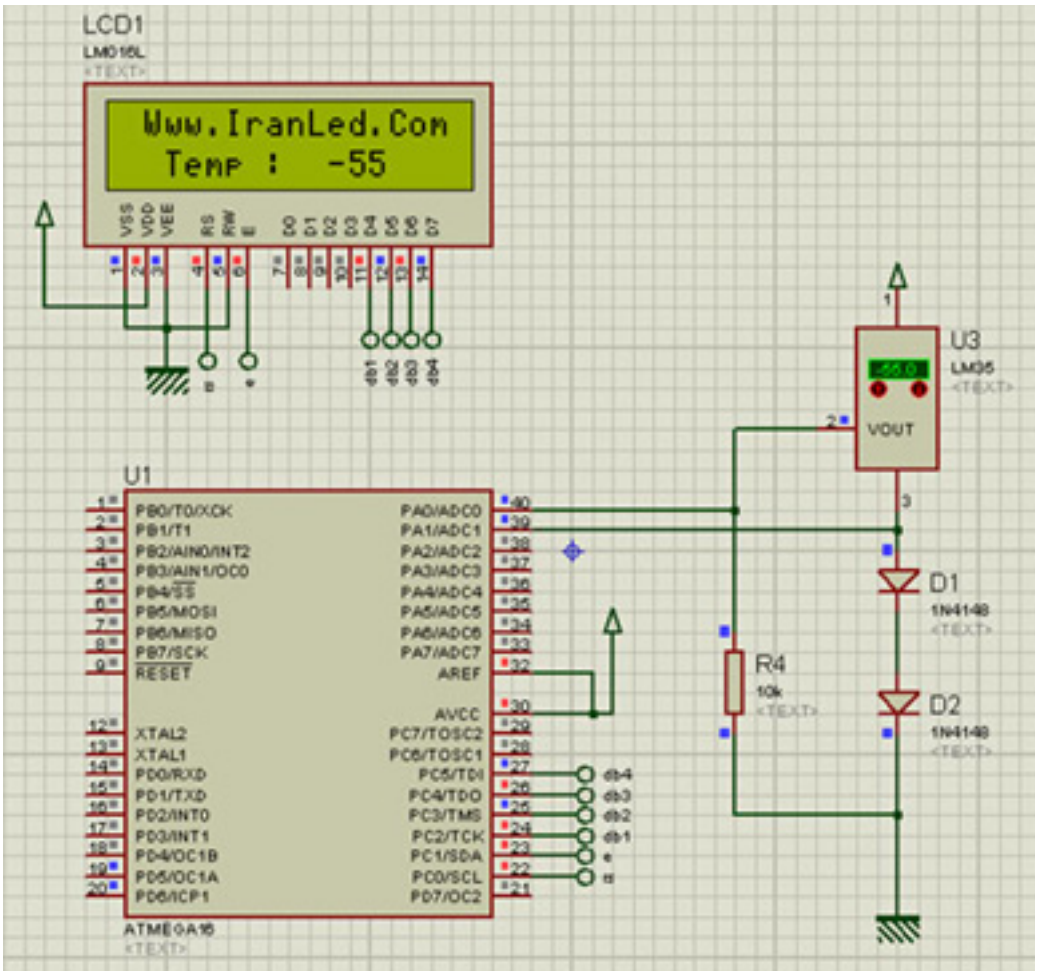
```
A = Getadc(0)
B = Getadc(1)
C = A - B
C = C / 2
S = Int(c)
```

در این قسمت ابتدا متغیر A بعنوان یکی از پایه های سنسور و متغیر B بعنوان پایه ای دیگر قرار داده شده اند و متغیر C برابر تفاضل A و B تقسیم بر ۲ و نهایتا به عدد صحیح تبدیل شده و در متغیر S قرار داده شده اند.

اکنون نوبت آن رسیده که دما را روی LCD به طریقه زیر نمایش دهیم؛

```
Locate 2 , 3
Lcd «Temp :  " ; S ; "  "
```

و اتمام برنامه.



فایهای مورد نیاز در پوشه Lm35 موجود است