

The main point in this article is about a change in compiler leads to generation of malicious binary code . For example C compiler is written in C and if someone add an additional if in the login part of OS cod the system could log with any string and we barely notice this vulnerability.

The learn phase is key point in this article because we should learn compiler to create our desire code (malicious cod) ...

If the compiler written in the source code language it is easy for us to hack it. We write the malicious compile in C (by adding some changes in correct version) and compile it by a correct compiler and put its binary instead of our compiler binary in OS.

Learning phase is shown by an example: first don't now tab and the second recognize it

```
...
c = next( );
if(c != '\\')
    return(c);
c = next( );
if(c == '\\')
    return('\\');
if(c == 'n')
    return('\n');
...
```

```
...
c = next( );
if(c != '\\')
    return(c);
c = next( );
if(c == '\\')
    return('\\');
if(c == 'n')
    return('\n');
if(c == 'v')
    return(11);
...
```

کامپایلر جدید با اضافه شدن خط
بنفش میتواند تب افقی را کامپایل
کند و در واقع بهش یاد دادیم

FIGURE 2.3.