

Use the utility **putty** to connect to F5 Management Interface, find the process ID which we want to attach

```
# ps aux | grep apd
root      351   kswapd0]
root      6246  runsv apd
root      6256  /usr/bin/apd -d 5 -f -n 20
root      18445 grep apd
```

We are interested in the one with ID **6256**.

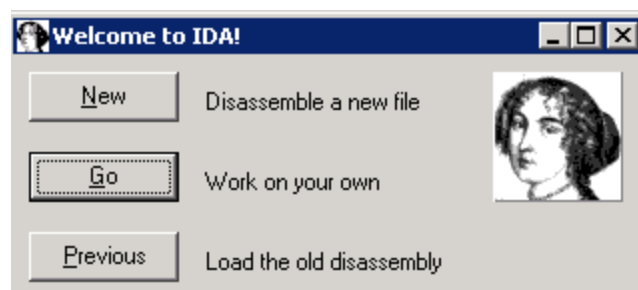
For remote debugging, you can totally use GDB without any problem. Here I'd like to take this opportunity to learn **IDA Debugger**(cross-platform).

Copy the file *linux_server* to the folder */shared/bin* on F5 VA.
Start the remote debug server on F5, you should see

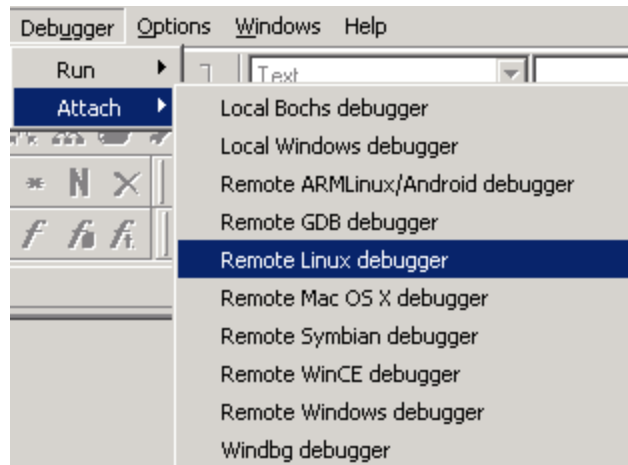
```
# /shared/bin/linux_server -Pmypass
IDA Linux 32-bit remote debug server(ST) v1.14. Hex-Rays (c) 2004-2011
Listening on port #23946...
```

Remember the listening port, we will use it below.

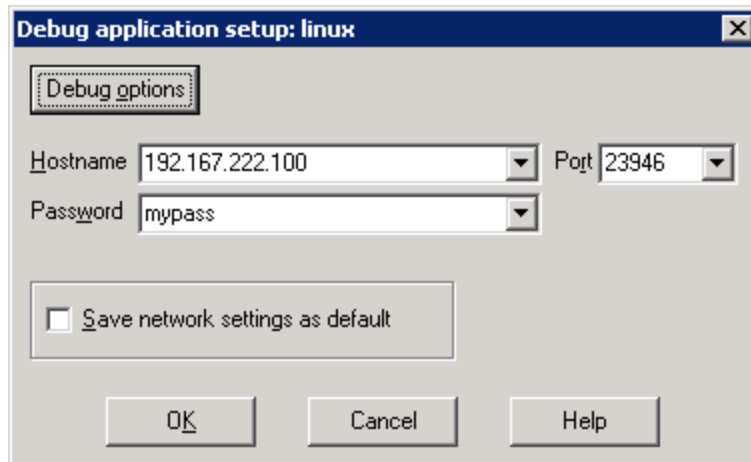
Start IDA Debugger, choose the button "Go"



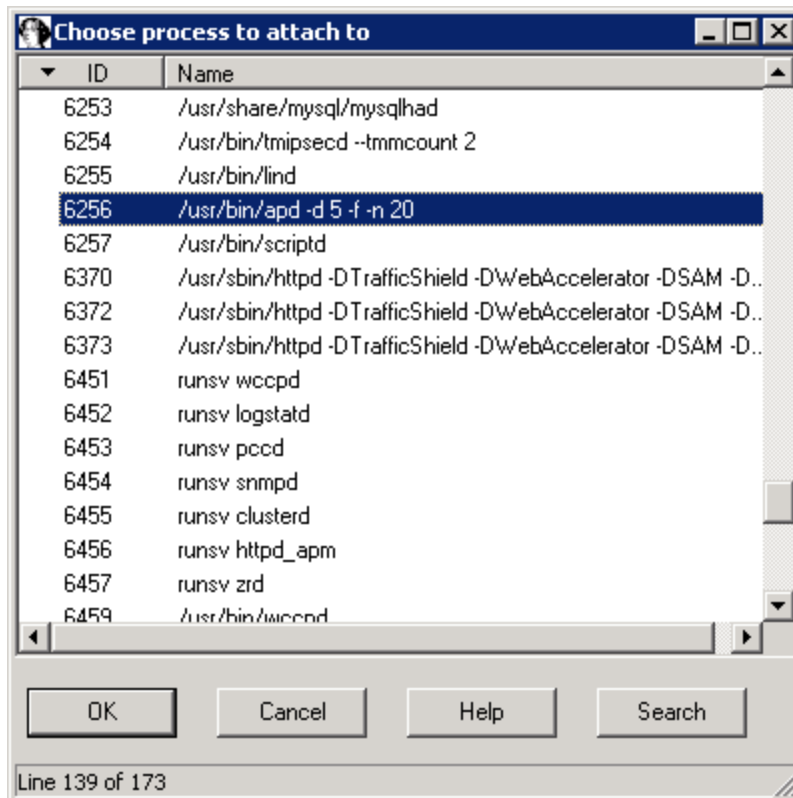
Then attach to the "Remote Linux Debugger"



It asks you where the remote debugger is (IP and port), also the password.

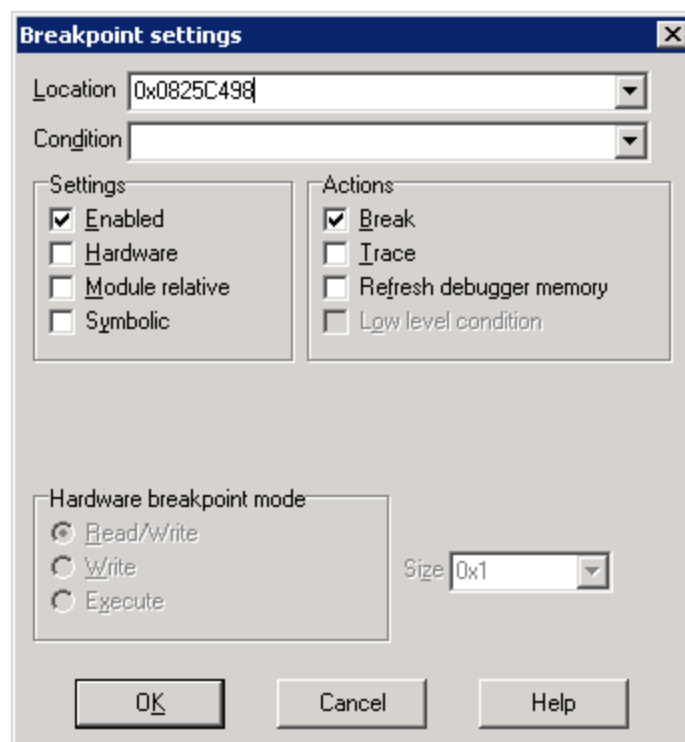


Then it lists all the processes running on the target machine. Find the ID we are interested in,



Attach to that process.

Add a breakpoint at 0x0825C498



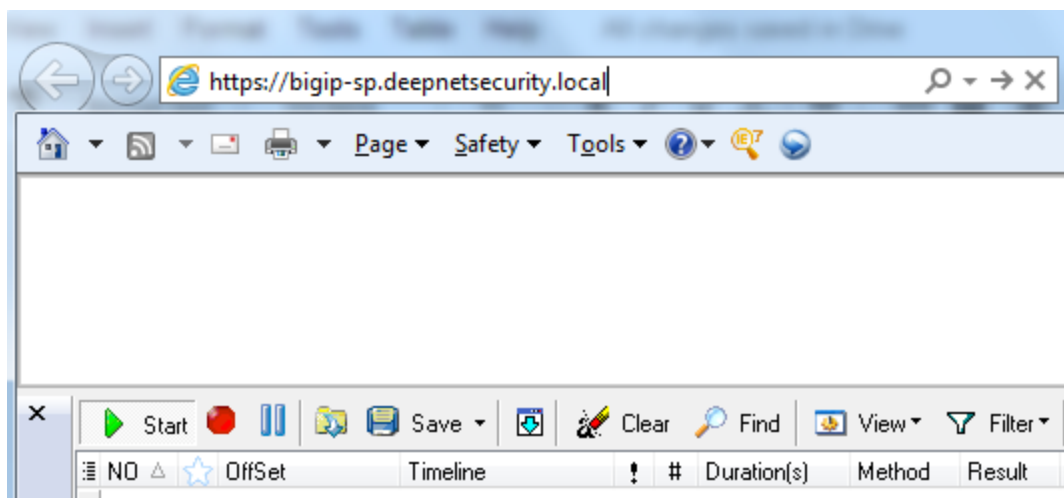
This is where the hash of canonical XML is computed and compared.

```

.text:0025C498 loc_825C498:                                     ; (
.text:0025C498                                             ; s
.text:0025C498 mov     eax, [ebp+var_14]
.text:0025C49B lea     ebx, [ebp+var_28]
.text:0025C49E mov     [esp+8], ebx
.text:0025C4A2 mov     [esp+4], eax
.text:0025C4A6 mov     eax, [ebp+var_10]
.text:0025C4A9 mov     [esp], eax
.text:0025C4AC call    _SHA1
.text:0025C4B1 cmp     [ebp+var_30], 14h
.text:0025C4B5 jnz     short loc_825C4CA
.text:0025C4B7 mov     edi, [ebp+var_3C]
.text:0025C4BA mov     ecx, 14h
.text:0025C4BF mov     esi, ebx
.text:0025C4C1 cld
.text:0025C4C2 repe    cmpsb
.text:0025C4C4 jz      loc_825C640

```

Now, install HTTP Watch(or HTTP Analyzer) IE add-on, open a browser, turn the recording on, then access the site published on F5.



Proceed SAML authentication until the process **apd** breaks at the configured breakpoint. Stop the recording, then find the content of SAMLResponse,

Parameter Name	Value
SAMLResponse	PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGlzZ0iVVRGLTgiF
RelayState	https://bigip-sp.deepnetsecurity.local

Save it to a file.

Go back to IDA Debugger,

After execution on 0825C498, check the register EAX, which equals to

0xD7B(=3451), I think it is the size of canonical XML content.

At 0825C4A9, EAX points to a buffer which contains the canonical XML content.
Check the memory area, and confirm I was right.

```
5B502B71 3C 73 61 6D 6C 70 3A 52 65 73 70 6F 6E 73 65 20 <samlp:Response
5B502B81 78 6D 6C 6E 73 3A 73 61 6D 6C 70 3D 22 75 72 6E xmlns:samlp="urn
5B502B91 3A 6F 61 73 69 73 3A 6E 61 6D 65 73 3A 74 63 3A :oasis:names:tc:
5B502BA1 53 41 4D 4C 3A 32 2E 30 3A 70 72 6F 74 6F 63 6F SAML:2.0:protoco
5B502BB1 6C 22 20 44 65 73 74 69 6E 61 74 69 6F 6E 3D 22 l" Destination="
5B502BC1 68 74 74 70 73 3A 2F 2F 62 69 67 69 70 2D 73 70 https://bigip-sp
5B502BD1 2E 64 65 65 70 6E 65 74 73 65 63 75 72 69 74 79 .deepnetsecurity
5B502BE1 2E 6C 6F 63 61 6C 2F 73 61 6D 6C 2F 73 70 2F 70 .local/saml/sp/p
5B502BF1 72 6F 66 69 6C 65 2F 70 6F 73 74 2F 61 63 73 22 rofile/post/acs"
5B502C01 20 49 44 3D 22 5F 39 35 32 33 65 34 62 66 39 61 ID="_9523e4bf9a
5B502C11 64 35 30 38 37 36 33 64 39 30 34 30 35 38 64 38 d508763d904058d8
5B502C21 65 62 35 32 64 34 35 61 35 37 64 33 66 38 22 20 eb52d45a57d3f8"
5B502C31 49 73 73 75 65 49 6E 73 74 61 6E 74 3D 22 32 30 IssueInstant="20
5B502C41 31 33 2D 30 35 2D 32 35 54 31 30 3A 32 36 3A 31 13-05-25T10:26:1
5B502C51 32 2E 38 32 38 5A 22 20 56 65 72 73 69 6F 6E 3D 2.8282" Version=
5B502C61 22 32 2E 30 22 3E 3C 73 61 6D 6C 32 3A 49 73 73 "2.0"><saml2:Iss
5B502C71 75 65 72 20 78 6D 6C 6E 73 3A 73 61 6D 6C 32 3D uer xmlns:saml2=
5B502C81 22 75 72 6E 3A 6F 61 73 69 73 3A 6E 61 6D 65 73 "urn:oasis:names
5B502C91 3A 74 63 3A 53 41 4D 4C 3A 32 2E 30 3A 61 73 73 :tc:SAML:2.0:ass
5B502CA1 65 72 74 69 6F 6E 22 3E 75 72 6E 3A 64 65 65 70 ertion">urn:deep
5B502CB1 6E 65 74 3A 64 75 61 6C 3A 69 64 70 3A 61 70 70 net:dual:idp:app
5B502CC1 73 73 6F 3C 2F 73 61 6D 6C 32 3A 49 73 73 75 65 sso</saml2:Issue
```

Dump the buffer to a file "canonical by F5.xml".

You can go further to 0825C4C1, it tries to compare the computed hash(stored in ESI) against the declared hash in **DigestValue**(stored in EDI).

```
ESI 5A2245F0  debug028:5A2245F0
EDI 0AA1EEA8  [heap]:0AA1EEA8
```

```
5A2245E0 00 00 00 00 44 0F 00 00 14 00 00 00 3E 0F 5F 58
5A2245F0 41 CB 20 3A FD 31 00 AD 1B 2C 80 2A 8A 9F 5A 60
5A224600 E2 0A 20 32 7B 0D 00 00 71 2B 50 5B B8 73 BF 0A
```

```
0AA1EEA8 38 9B 19 4E 59 45 0F C2 79 A0 52 2C 9B FA 89 85
0AA1EEB8 E1 28 71 47 00 C9 6E 00 20 00 00 00 11 00 00 00
```

Use MS utility FCIV to double check the hash on file "canonical by F5.xml"

```
fciv.exe -sha1 "canonical by F5.xml"
//
// File Checksum Integrity Verifier version 2.05.
//
41cb203afd3100ad1b2c802a8a9f5a60e20a2032 canonical by f5.xml
```

Use online utility to decode base64 value of **DigestValue**. The result is exact same to the value stored on EDI.

base64-encoding.online-domain-tools.com/tool-form-submit/

P A... Trotters and Tales: P... Fast I1 Minimization... mrtazz/restclient-c

Base64 – Online Encoders and Decoders

Tool: Base64 Encoder/Decoder

Input type: Text

Input text: OJs2T11FD8J5oFIsm/gJheEocUc=

> Encode! > Decode!

Decoded input:

00000000	38 9b 19 4e 59 45 0f c2 79 a0 52 2c 9b fa 89 85
00000010	e1 28 71 47

Now use **Apache Santuario** utility *checksig* to dump the canonical XML content from the same SAML response, and use FCIV to calculate its SHA1 hash. Very pleasing, it is identical to the one decoded from **DigestValue**.

```
fciv.exe -sha1 "canonical by Apache.xml"
//
// File Checksum Integrity Verifier version 2.05.
//
389b194e59450fc279a0522c9bfa8985e1287147 canonical by apache.xml
```

Let us focus on two XML elements. In the original SAML response (decoded to XML), we have the first one,

```
<samlp:Response Destination=
"https://bigip-sp.deepnetsecurity.local/saml/sp/profile/post/acs" ID=
"_9523e4bf9ad508763d904058d8eb52d45a57d3f8" IssueInstant="2013-05-25T10:26:12.828Z"
Version="2.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml=
"urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp=
"urn:oasis:names:tc:SAML:2.0:protocol"><saml2:Issuer xmlns:saml2=
```

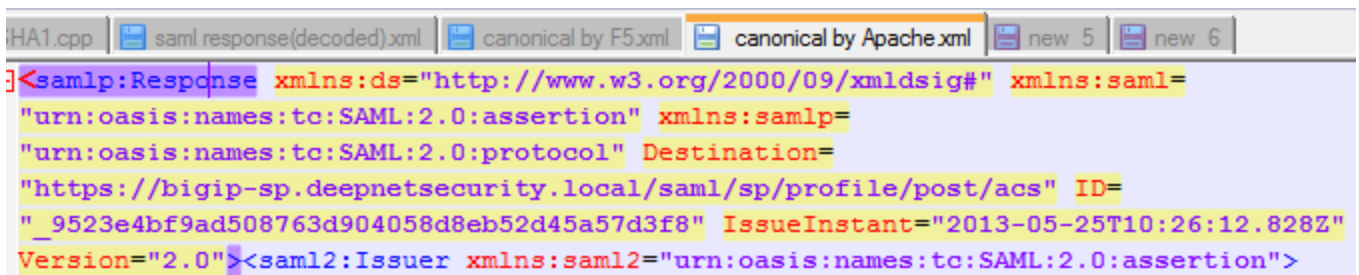
which has 7 attributes.

And the second one

```
</samlp:Status><saml:Assertion ID="_72791fdf2de3fb7ea0692fcfc78a318b75c4daf4"
IssueInstant="2013-05-25T10:26:12.828Z" Version="2.0"><saml2:Issuer xmlns:saml2=
```

which has 3 attributes.

In **canonical by apache.xml**, we have,



```
<samlp:Response xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml=
"urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp=
"urn:oasis:names:tc:SAML:2.0:protocol" Destination=
"https://bigip-sp.deepnetsecurity.local/saml/sp/profile/post/acs" ID=
"_9523e4bf9ad508763d904058d8eb52d45a57d3f8" IssueInstant="2013-05-25T10:26:12.828Z"
Version="2.0"><saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

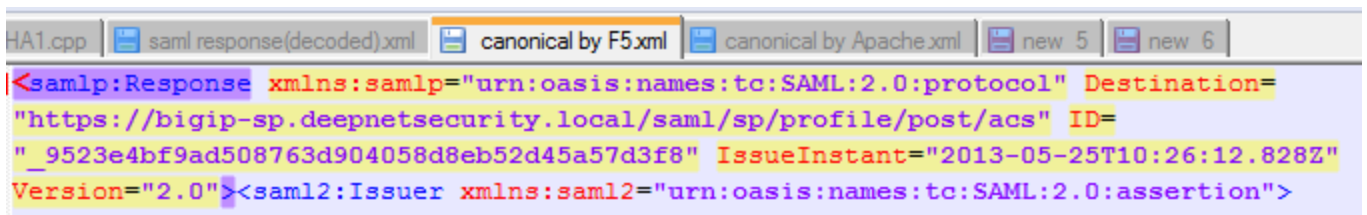
It still has 7 attributes, although they are reordered which is expected.

For the second element,

```
</samlp:Status><saml:Assertion ID="_72791fdf2de3fb7ea0692fcfc78a318b75c4daf4"
IssueInstant="2013-05-25T10:26:12.828Z" Version="2.0"><saml2:Issuer xmlns:saml2=
```

The amount of attributes is still same, which is three.

However, in **canonical by F5.xml**, we have,



```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination=
"https://bigip-sp.deepnetsecurity.local/saml/sp/profile/post/acs" ID=
"_9523e4bf9ad508763d904058d8eb52d45a57d3f8" IssueInstant="2013-05-25T10:26:12.828Z"
Version="2.0"><saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

It missed two attributes on this element.

```
</samlp:Status><saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID=
"_72791fdf2de3fb7ea0692fcfc78a318b75c4daf4" IssueInstant="2013-05-25T10:26:12.828Z"
Version="2.0"><saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

It coined out a new attribute on this one.

