

Website Monitoring - Bug #1558

NTLM authentication fails because MD4 is not available

11/09/2016 12:10 AM - Luke Murphey

Status:	Closed	Start date:	11/09/2016
Priority:	Normal	Due date:	
Assignee:	Luke Murphey	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	2.0.1		
Description			
<a href="https://answers.splunk.com/answers/469223/is-it-possible-to-switch-to-windows-authentication.html">https://answers.splunk.com/answers/469223/is-it-possible-to-switch-to-windows-authentication.html</a>			

History

#1 - 11/09/2016 12:10 AM - Luke Murphey

```
import hashlib
m = hashlib.new('md4')
```

#2 - 11/09/2016 12:11 AM - Luke Murphey

Splunk only supports: ('md5', 'sha1', 'sha224', 'sha256', 'sha384', 'sha512')

```
import hashlib
hashlib.algorithms
```

#3 - 11/09/2016 12:14 AM - Luke Murphey

Related:

- [https://bugzilla.redhat.com/show\\_bug.cgi?id=1295459](https://bugzilla.redhat.com/show_bug.cgi?id=1295459)

#4 - 11/09/2016 12:18 AM - Luke Murphey

Odd, this is the call that fails but that should work on my host:

```
digest = hashlib.new('md4', passwd.encode('utf-16le')).digest()
```

This works on my host:

```
bin/splunk cmd python -c "import hashlib;print hashlib.new('md4', 'test').hexdigest()"
```

That prints: db346d691d7acc4dc2625db19f9e3f52

#### #5 - 11/09/2016 05:19 AM - Luke Murphey

This didn't work for me on Windows 10 Pro with Splunk 6.5 (Python 2.7.11).

#### #6 - 11/09/2016 05:29 AM - Luke Murphey

The unit tests fail on Windows but pass on \*nix.

#### #7 - 12/05/2016 11:32 PM - Luke Murphey

- Assignee set to Luke Murphey
- Target version set to 2.0.1

#### #8 - 12/05/2016 11:33 PM - Luke Murphey

See:

- <https://gist.github.com/tristanwietsma/5937448>
- <https://gist.github.com/bonsaiviking/5644414>

#### #9 - 12/06/2016 01:10 AM - Luke Murphey

They are returning the same value but the custom implementation returns a hex array string.

#### #10 - 12/06/2016 01:31 AM - Luke Murphey

- Status changed from New to Closed
- % Done changed from 0 to 100

#### #11 - 12/06/2016 03:28 AM - Luke Murphey

```
import hashlib
from md4 import MD4

def hash_md4(data):
    md4 = MD4()
    md4.update(data)
    return md4

def hash_md4_orig(data):
    return hashlib.new('md4', data)

d = "tree"
new = hash_md4(d).digest()
expected = '\xb6\x84+C\xe7L$\xbbM\x14\xd2N\xd5\x10d\xcb'

if new == expected:
    print "hash matches"
else:
    print "hash does not match"

orig = hash_md4_orig(d).digest()

if orig == expected:
    print "orig hash matches"
else:
    print "orig hash does not match"
```

**#12 - 12/06/2016 04:32 AM - Luke Murphey**

- *Status changed from Closed to In Progress*

This works on my mac but I get a different hash on Windows.

**#13 - 01/06/2017 07:48 PM - Luke Murphey**

- *Status changed from In Progress to Closed*

**#14 - 08/12/2017 03:32 AM - Luke Murphey**

<https://stackoverflow.com/questions/22224840/use-python-mechanize-to-log-into-pages-with-ntlm-authentication>