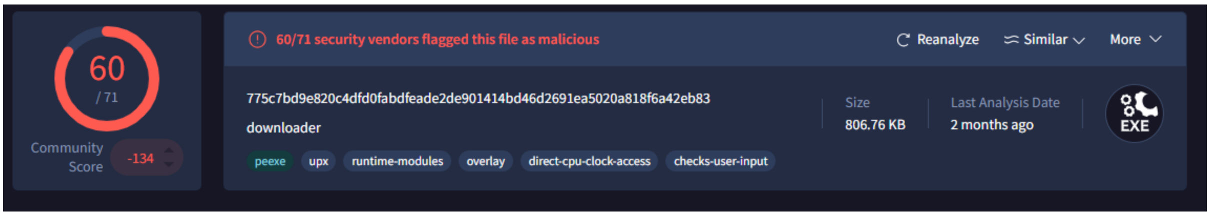
Name: Chanchal Teli

Intern ID:125

Malware Analysis

Malware: 'Adware (004f7c2e1) 'Adware (004f7c2e1)

Hash: 775c7bd9e820c4dfd0fabdfeade2de901414bd46d2691ea5020a818f6a42eb83



60 / 71

Community Score -134

60/71 security vendors flagged this file as malicious

775c7bd9e820c4dfd0fabdfeade2de901414bd46d2691ea5020a818f6a42eb83

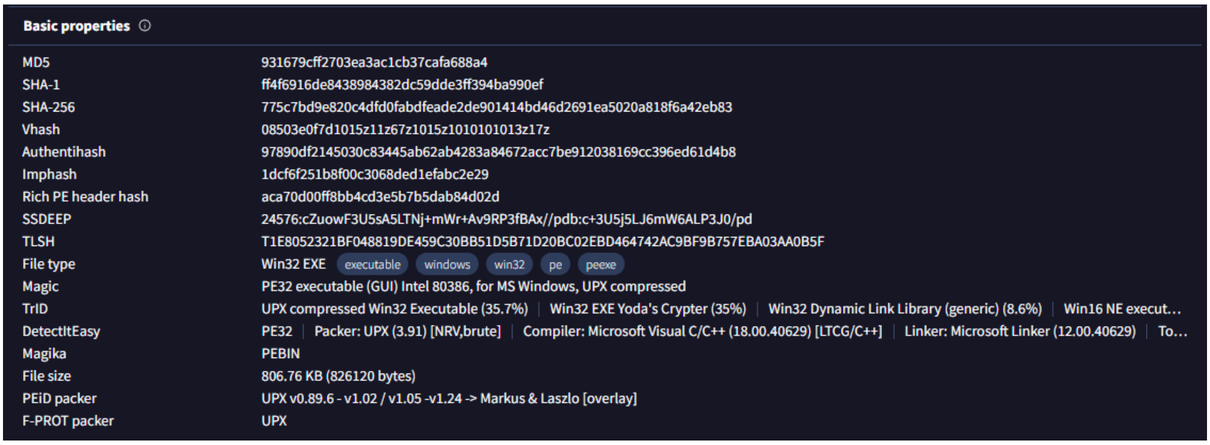
downloader

peexe upx runtime-modules overlay direct-cpu-clock-access checks-user-input

Size 806.76 KB

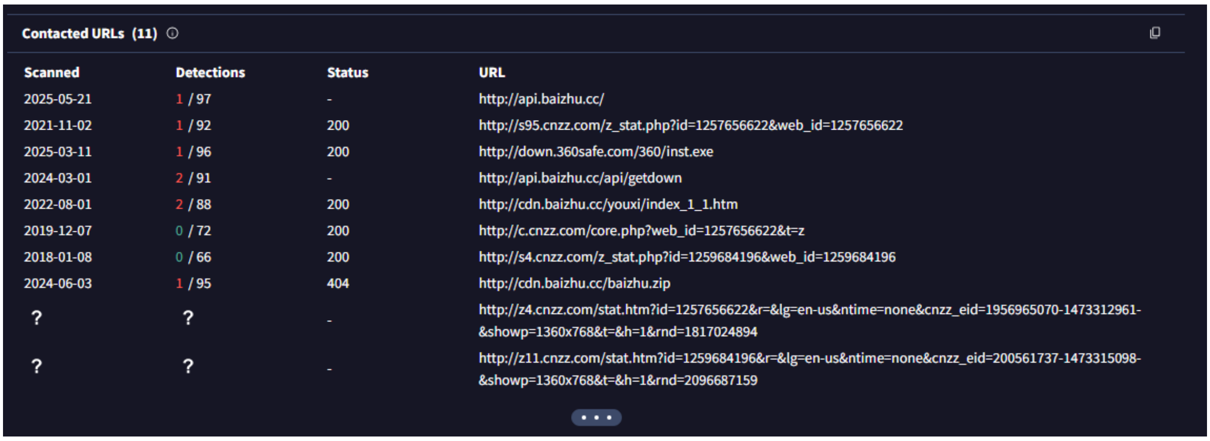
Last Analysis Date 2 months ago

Basic Properties:



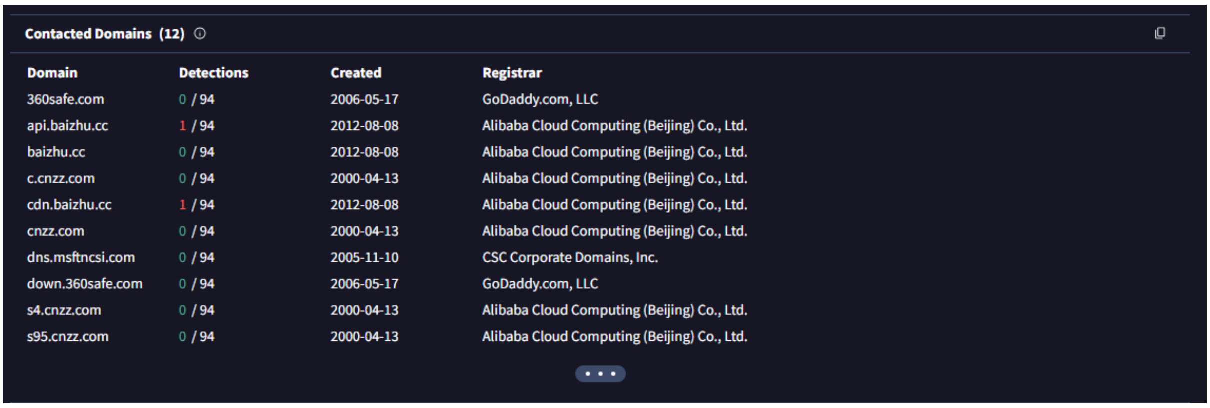
Basic properties

MD5	931679cff2703ea3ac1cb37cafa688a4
SHA-1	ff4f6916de8438984382dc59dde3ff394ba990ef
SHA-256	775c7bd9e820c4dfd0fabdfeade2de901414bd46d2691ea5020a818f6a42eb83
Vhash	08503e0f7d1015z11z67z1015z1010101013z17z
Authentihash	97890df2145030c83445ab62ab4283a84672acc7be912038169cc396ed61d4b8
Imphash	1dcf6f251b8f00c3068ded1efabc2e29
Rich PE header hash	aca70d00ff8bb4cd3e5b7b5dab84d02d
SSDEEP	24576:cZuowF3U5sA5LTNj+mWr+Av9RP3fBAx//pdb:c+3U5j5LJ6mW6ALP3J0/pd
TLSH	T1E8052321BF048819DE459C30BB51D5B71D20BC02EBD464742AC9BF9B757EBA03AA0B5F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
TrID	UPX compressed Win32 Executable (35.7%) | Win32 EXE Yoda's Crypter (35%) | Win32 Dynamic Link Library (generic) (8.6%) | Win16 NE execut…
DetectItEasy	PE32 | Packer: UPX (3.91) [NRV,brute] | Compiler: Microsoft Visual C/C++ (18.00.40629) [LTCG/C++] | Linker: Microsoft Linker (12.00.40629) | To…
Magika	PEBIN
File size	806.76 KB (826120 bytes)
PEiD packer	UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]
F-PROT packer	UPX



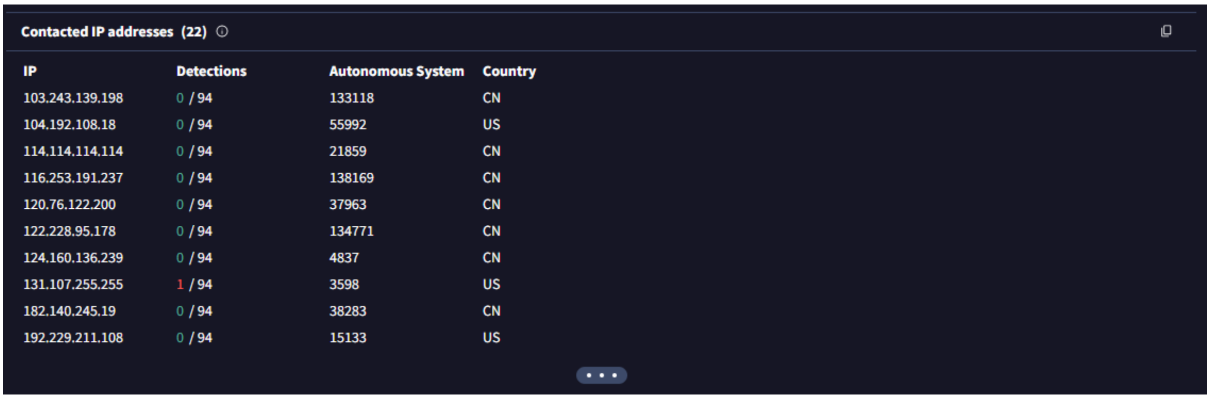
Contacted URLs (11)

Scanned	Detections	Status	URL
2025-05-21	1 / 97	-	http://api.baizhu.cc/
2021-11-02	1 / 92	200	http://s95.cnzz.com/z_stat.php?id=1257656622&web_id=1257656622
2025-03-11	1 / 96	200	http://down.360safe.com/360/inst.exe
2024-03-01	2 / 91	-	http://api.baizhu.cc/api/getdown
2022-08-01	2 / 88	200	http://cdn.baizhu.cc/youxi/index_1_1.htm
2019-12-07	0 / 72	200	http://c.cnzz.com/core.php?web_id=1257656622&t=z
2018-01-08	0 / 66	200	http://s4.cnzz.com/z_stat.php?id=1259684196&web_id=1259684196
2024-06-03	1 / 95	404	http://cdn.baizhu.cc/baizhu.zip
?	?	-	http://z4.cnzz.com/stat.htm?id=1257656622&r=&lg=en-us&ntime=none&cnzz_eid=1956965070-1473312961-&showp=1360x768&t=&h=1&rnd=1817024894
?	?	-	http://z11.cnzz.com/stat.htm?id=1259684196&r=&lg=en-us&ntime=none&cnzz_eid=200561737-1473315098-&showp=1360x768&t=&h=1&rnd=2096687159



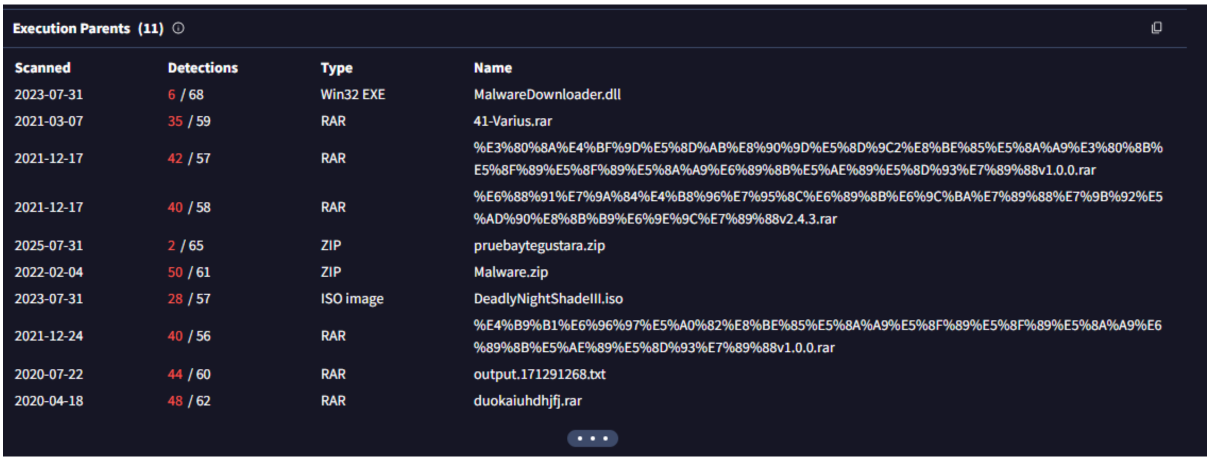
Contacted Domains (12)

Domain	Detections	Created	Registrar
360safe.com	0 / 94	2006-05-17	GoDaddy.com, LLC
api.baizhu.cc	1 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
baizhu.cc	0 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
c.cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.
cdn.baizhu.cc	1 / 94	2012-08-08	Alibaba Cloud Computing (Beijing) Co., Ltd.
cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.
dns.msftncsi.com	0 / 94	2005-11-10	CSC Corporate Domains, Inc.
down.360safe.com	0 / 94	2006-05-17	GoDaddy.com, LLC
s4.cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.
s95.cnzz.com	0 / 94	2000-04-13	Alibaba Cloud Computing (Beijing) Co., Ltd.



Contacted IP addresses (22)

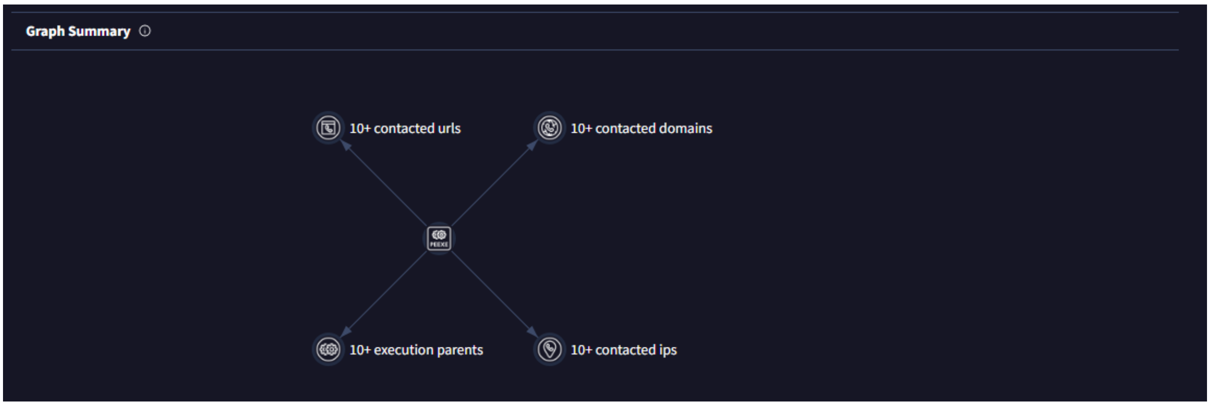
IP	Detections	Autonomous System	Country
103.243.139.198	0 / 94	133118	CN
104.192.108.18	0 / 94	55992	US
114.114.114.114	0 / 94	21859	CN
116.253.191.237	0 / 94	138169	CN
120.76.122.200	0 / 94	37963	CN
122.228.95.178	0 / 94	134771	CN
124.160.136.239	0 / 94	4837	CN
131.107.255.255	1 / 94	3598	US
182.140.245.19	0 / 94	38283	CN
192.229.211.108	0 / 94	15133	US



Execution Parents (11)

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2021-03-07	35 / 59	RAR	41-Varius.rar
2021-12-17	42 / 57	RAR	%E3%80%8A%E4%BF%9D%E5%8D%AB%E8%90%9D%E5%8D%9C2%E8%BE%85%E5%8A%A9%E3%80%8B%E5%8F%89%E5%8F%89%E5%8A%A9%E6%89%8B%E5%AE%89%E5%8D%93%E7%89%88v1.0.0.rar
2021-12-17	40 / 58	RAR	%E6%88%91%E7%9A%84%E4%B8%96%E7%95%8C%E6%89%8B%E6%9C%BA%E7%89%88%E7%9B%92%E5%AD%90%E8%8B%B9%E6%9E%9C%E7%89%88v2.4.3.rar
2025-07-31	2 / 65	ZIP	pruebaytegustara.zip
2022-02-04	50 / 61	ZIP	Malware.zip
2023-07-31	28 / 57	ISO image	DeadlyNightShadeIII.iso
2021-12-24	40 / 56	RAR	%E4%B9%B1%E6%96%97%E5%A0%82%E8%BE%85%E5%8A%A9%E5%8F%89%E5%8F%89%E5%8A%A9%E6%89%8B%E5%AE%89%E5%8D%93%E7%89%88v1.0.0.rar
2020-07-22	44 / 60	RAR	output.171291268.txt
2020-04-18	48 / 62	RAR	duokaiuhdhjfj.rar

Graph:



Identifying Available Shares on Windows Systems

Activity Overview

This guide explains how to identify and analyze shared resources on a Windows system using the built-in net share command.

The net share Command

The net share command is a Windows shell command that displays information about all resources being shared on the local computer. This includes:

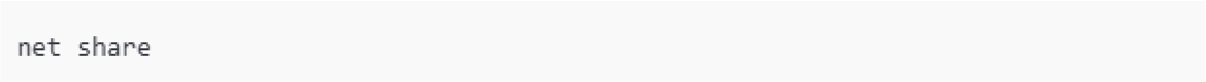
- File system directories
- Printers
- Administrative shares

Basic Usage

1. Open Command Prompt or PowerShell:

- Press Win + R to open the Run dialog.
- Type cmd and press Enter (or type powershell for PowerShell).

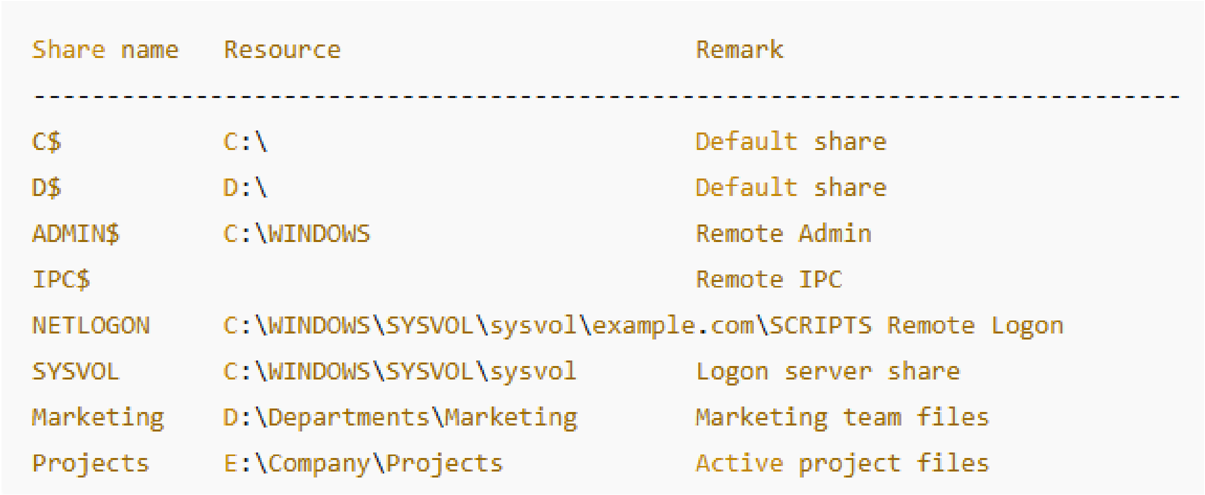
2. Run the Command:



```
net share
```

3. Press Enter to execute the command.

Output



```
Share name   Resource                        Remark
-------------------------------------------------------------------------------
C$           C:\                             Default share
D$           D:\                             Default share
ADMIN$       C:\WINDOWS                      Remote Admin
IPC$                                         Remote IPC
NETLOGON     C:\WINDOWS\SYSVOL\sysvol\example.com\SCRIPTS Remote Logon
SYSVOL       C:\WINDOWS\SYSVOL\sysvol        Logon server share
Marketing    D:\Departments\Marketing        Marketing team files
Projects     E:\Company\Projects             Active project files
```

Understanding the Output

Field	Description
Share name	The name that network users see when browsing shared resources
Resource	The local path of the shared folder or resource
Remark	A description or comment about the shared resource

Common Default Shares

Share	Purpose
C$, D$	Administrative shares for each drive letter (hidden by default)
ADMIN$	Points to the Windows directory
IPC$	Used for inter-process communication
NETLOGON	Domain logon scripts
SYSVOL	Domain policies and scripts

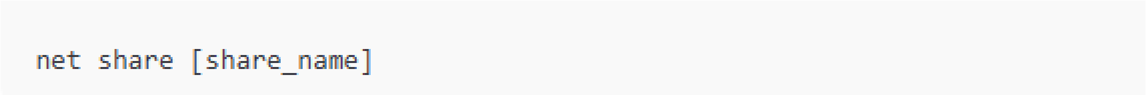
Security Implications

Using net share helps identify:

- Oversharing: Unnecessary n
- etwork-exposed folders
- Default shares: Should be monitored or disabled if not required
- Unauthorized shares: Detect unknown or risky share entries

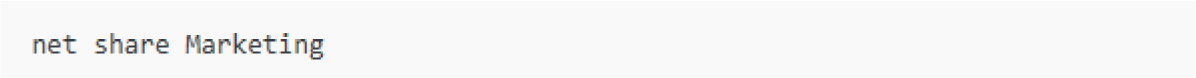
Advanced Usage

1. Get Detailed Info About a Share:



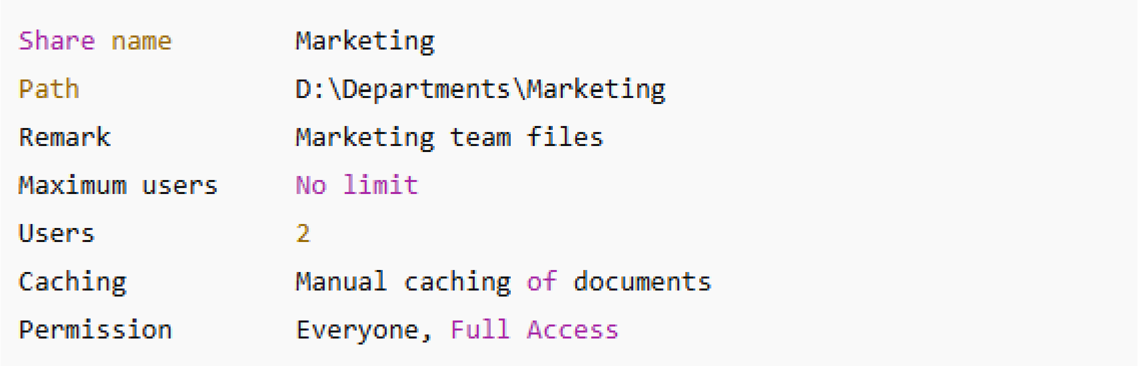
```
net share [share_name]
```

Example:



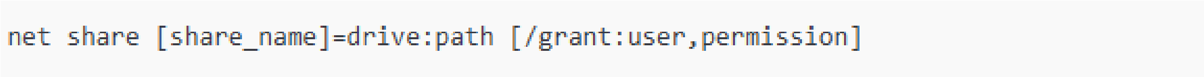
```
net share Marketing
```

Output:



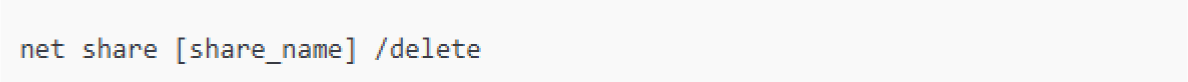
```
Share name         Marketing
Path               D:\Departments\Marketing
Remark             Marketing team files
Maximum users      No limit
Users              2
Caching            Manual caching of documents
Permission         Everyone, Full Access
```

2. Create a New Share:



```
net share [share_name]=drive:path [/grant:user,permission]
```

3. Remove a Share:



```
net share [share_name] /delete
```

Security Use Cases

Audit Network Exposure

- Identify folders accessible to others over the network
- Detect sensitive folders (e.g., containing credentials, reports) shared publicly

Detect Unauthorized Shares

- Look for unfamiliar share names like backup$, temp, hidden, etc.
- Check for shared locations such as C:\Users\Admin\Downloads

Investigate Default Shares

- C$, D$, ADMIN$, IPC$ are hidden administrative shares
- These can be misused if weak credentials are used

Conclusion

The net share command offers a quick and effective way to view and manage shared resources on a Windows system. It helps identify default, authorized, and unauthorized shares, making it valuable for both system administration and security auditing. Regular use of this command supports better control and protection of shared data.