


Threat Level: **GREEN**

Handler on Duty: **Xavier Mertens**



InfoSec Handlers Diary Blog

Keyword, Domain, Port, IP or Header

Email Password
[Sign Up for Free!](#) [Forgot Password?](#)

Contact Us

DIARY

Podcasts

Jobs

News

Tools

Data

Forums

/tmp, %TEMP%, ~/Desktop, T:\, ... A goldmine for pentesters!

Published: 2016-01-20

Last Updated: 2016-01-20 10:06:25 UTC

by [Xavier Mertens](#) (Version: 1)

2 comment(s)

When you are performing a penetration test, you need to learn how your target is working: What kind of technologies and tools are used, how internal usernames are generated, email addresses format, ... Grabbing for such information is called the reconnaissance phase. Once you collected enough details, you can prepare your different scenarios to attack the target. All pentesters have their personal toolbox that has been enhanced day after day. In many cases, there is no real magic: to abuse or get around a security control "x", use the tool "y". But there is also a question of chance... Lucky people can discover security issues "by chance". This also applies to bad guys.

A goldmine for the pentester are temporary directories. Almost all software use temporary files to perform their tasks. Users like to use them to exchange files with colleagues. I'll give you two real examples:

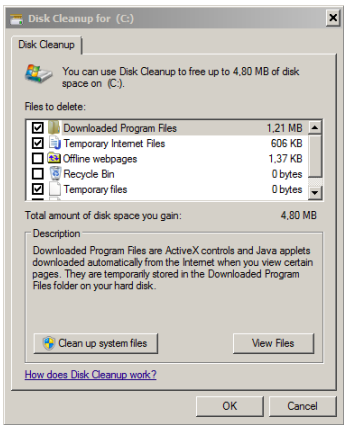
In a recent mission, I took control of a workstation connected to the Windows domain then I started to collect juicy data by browsing all the fileshares. The customer implemented access controls and access to files was restricted at group level (Example: only the IT team was able to access the "I:" drive containing technical documentation about the infrastructure). However, some people exchanged IT related files via the "T:" share and they were still available during the pentest.

Another one? When pivoting from workstation to workstation on a LAN, I discovered a screenshot on a user's desktop. This screenshot was a domain controller admin page which listed all the domain administrators. I just had to track them and, once a valid session found, to extract the user's password with [Mimikatz](#) to get domain admin privileges.

On Linux systems, the /tmp directory is usually cleaned at boot time or via a cron (files older than x days are removed) but other places like /var/tmp, /usr/local/tmp are not cleaned by default! It is easy to schedule the following command at regular interval. It will delete files from /tmp that haven't be modified for more than 7 days.

```
# find /tmp -mtime +7 -exec rm -rf {} \;
```

On Ubuntu, files in /tmp are cleaned at book time via the variable TMPTIME= in /etc/default/rcS. Be sure to check your Linux distribution to know how it takes care of /tmp. For Windows, it's even worse, there is no automatic deletion of files stored in %TEMP%. The Disk Cleaner tool can delete files but it is started when the disk space is going too low:



An easy way to automate this task is to create a small script and execute it at your best convenience (at boot time or at regular interval via a scheduled task):

```
rd %TEMP% /s /q
md %TEMP%
```

There exist plenty of tools which also take care of temporary files like [CCleaner](#). To clean up files on a temporary fileshare, Powershell is helpful:

```
PS C:\> $days = (Get-Date).AddDays(-7)
PS C:\> $path = "T:\\"
PC C:\> Get-ChildItem -Path $path -Recurse -Force | Where-Object { !$_.PSIsContainer -and
```

Some best practices:

- By definition, temporary files must have a very short life time.
- Do NOT share sensitive data via fileshares (database dumps, backups, passwords lists, ...)
- Once you finished to work with temporary files, don't forget to delete them.
- If you need to exchange files with colleagues via a shared folder, keep in mind that often other people could read them.
- Change the permissions to restrict access to authorized users/groups only via chmod / chown on UNIX or icacls on Windows (or the GUI).
- Encrypt sensitive data (internally, a password protected zip file will be enough in most cases).
- On Unix, use [umask](#) to change the default permissions of created files.

Xavier Mertens

ISC Handler – Freelance Security Consultant

[PGP Key](#)

Keywords: [fileshare](#) [pentesting](#) [temporary files](#) [tmp](#)

2 comment(s)

Join us at SANS! [SANS SEC503: Intrusion Detection In-Depth. Gain the technical knowledge, insight, and hands-on training you need to defend your network with confidence.](#)

[previous](#)

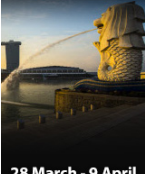
[Top of page](#)

[Diary Archives](#)

SANS

Secure Singapore 2016

Largest & Most Exciting Course Lineup in APAC region to date!



28 March - 9 April

[LEARN MORE](#)

https://isc.sans.edu/diary/tmp%2C+%25TEMP%25%2C+~/Desktop%2C+T%3A%5C%2C+...+A+goldmine+for+pentesters%21/20631

1/2

