System Resource 定義: 範例 (2/2)

- Example of OS configuration file:

File name	File description	Exploit usage
/etc/ftpusers	Provides user access control for ftpd (*file transfer protocol daemon*).	Exfiltration (T1048)
/etc/crontab	Contains information on what system jobs are run by cron.	Scheduled Task/Job (T1053)
/etc/hosts	Mappings of IP addresses to host names.	DNS Spoofing (T1584)

- Notes: not all configuration files are located in the /etc/ directory. Some configuration files may be located in other directories such as /usr/share/. However, we exclude such directories since they are not attack-related.

Directory name	Directory description
/usr/share/applications/	Contains desktop application launcher files used by various Linux desktop environments such as GNOME and KDE.
/usr/share/icons/	Contains icon themes used by various applications.

Subsolution #1c – Operations that Change System State

- In Subsolution #2b, we define and list the OS configuration file.
- We still need to define what operations (system calls) will change the OS system state by modifying any file objects.
  - Object: Any file entity type objects. (e.g. /var/readme, /etc/rc.local)
  - Action: The system call should belongs to the category File::Upate (37個) & File::Delete (8個) that will be define in Subsolution #3a. (e.g. rm(), write())
  - 須注意的是在 Linux OS 下許多檔案是虛擬的即時生成出來的 (pseudo-filesystem)，實際上並無此檔案的存在，因次也不存在修改虛擬檔案的操作。(e.g. /proc/, /sys/)
- 系統設定檔和改變系統環境是獨立的。