IT3789 Cyber Security Attack & Defence

L13 – Covering Tracks

WITH KNOWLEDGE COMES RESPONSIBILITY

Overview

- In profession penetration testing, covering tracks is a step that is usually not done.
- Purpose
  - To understand where obstacles exists.
  - To fully understand the security posture of the target.

Covering Tracks

Manipulating Log Data

Hiding Files

Covering Tracks and Erasing Evidence

- After attackers gained administrator access, they try to cover their tracks to prevent detection on the system.
  - Avoid detection.
  - Continue using owned system.
    - e.g. Hiding backdoor.
  - Remove evidence of attack including attacker identity and activities.
  - Possibly avoid legal actions.
- Two methods of covering tracks.
  - Disable auditing on the system.
  - Manipulate log data.

Manipulating Log Data

- System administrators watch for malicious activities by examining log files.
- Two general types of log files
  - System-generated
  - Application-generated
- Two options when manipulating log data.
  - Delete the entire log.
  - Modify the contents of the log file.
- Remember that the ultimate objective is to be stealth.

Delete Log File

- Removing the log file from the system.
- Advantage
  - Once log file is removed, it will be difficult to trace the attack on the system.
    - Good for hiding the identity of the attacker and where he comes from.
- Drawback
  - The chance of detection of the attack is higher as it is pretty obvious that the log file is "gone".
    - Note that log file exists not only to detect malicious activities but also to determine state and health of system.

Modify Contents of Log File

- To hide attack attempts on the system, log data related to the attack are removed.
- Advantage
  - When a system administrator examines the log file, it is harder for them to find any anomalies.
- Drawbacks
  - May miss out some events that are related to the attack.
  - May leave gaps in the log that will be noticeable.

Manipulating Log Data

- Note that system administrator can store log files in remote servers.
- When remote log servers exist, there are two ways to manipulate log data.
  1. Shutdown the log data transfer process.
  2. Attack the remote log servers.
- There may be alarms on the log server which will be triggered when log transfer is interrupted.

Covering Tracks

Manipulating Log Data

Hiding Files

Hiding Files

- During penetration testing, files and scripts may be needed to be uploaded to the exploited system.
  - e.g. To make a backdoor permanent, the hacker may create a script and make it launch every time the system reboots.
- If administrator discovers these scripts, the attack will be stopped.
  - Files can be hidden in plain sight or using the operating system file structure.

Hiding Files in Windows

- Two ways to hide files in Windows:
  - The attrib command.
  - Alternate Data Streams in NTFS file system.
- To hide file using the attrib command, type the following at the command prompt.

```
attrib + h [file/directory]
```

Hiding Files in Windows

- Alternate Data Streams (ADS) allows a hidden file to be hidden in a legitimate file.
- Features in ADS
  - The hidden file will not appear in a directory listing.
    - A user will not normally suspect the legitimate file that appears in the directory listing.
  - Allows creation of many ADS under the same filename.
  - ADS is able to hide directory too!
- Limitation of ADS
  - Only works on NTFS file systems.

Hiding Files in Windows

- makestrm.exe is a utility that can move data from a file to an ADS.
- Executable files can be hidden in ADS as well.
  - This means malwares and viruses can be hidden in ADS.
  - Executable files can be run directly from the ADS.
- Some scanners do not scan ADS for any malware or virus.

ADS Countermeasures

- Tools for finding alternate data streams in NTFS
  - LADS (List Alternate Data Streams) by Frank Heyne.
    - Command line tool that scans drives or a given directory for ADS.
    - http://www.heysoft.de/en/information/ntfs-ads.php?lang=EN
  - LNS (List NTFS Streams) is a tool that detects NTFS streams.
    - Reports the existence and location of file that contains ADS.
    - http://www.ntsecurity.nu/toolbox/lns/

Hiding Files and Directories in UNIX

- Store files in /tmp directory which is usually erased at reboot
- Using dots as filenames to hide files.
  - ". " (dot-space)
  - ".. " (dot-dot-space)
  - Usually administrator will miss them
  - Countermeasure: Use the following to locate these files.

```
# find / -name ". "
# find / -name ".. "
```

Hiding Files and Directories in UNIX

- Using dots as filenames to hide files. (cont'd)
  - The file does not show by using ls to list the directory.

```
root@bt:~# ls
Ex01  Ex04  Ex07  Ex11  Ex15      Launch Leo.desktop  pwbv3
Ex02  Ex05  Ex08  Ex12  Exploits  Report              tools
Ex03  Ex06  Ex09  Ex13  Info      Resources
```

```
root@bt:~# ls -a
.                   .gem                .pbnj-2.0           Ex06
..                  .gnome2             .profile            Ex07
..                  .gnome2_private     .qt                 Ex08
 DCOPserver_bt_:0   .gtk.qt.engine.rc   .recently-used.xbel  Ex09
```

Covering Tracks

Manipulating Log Data

- Delete Log File
- Modify Log Data

Hiding Files

- Hiding Files in Windows
- Hiding Files in Unix