8.4.4 Cover Your Tracks Facts

Covering tracks is an important phase in hacking to prevent being traced and to remain undetected during continued access. There are many methods hackers use to remove traces of their attacks.

This lesson covers the following topics:

- Erase or modify evidence
- Hide evidence
- Modify timestamps
- Disable auditing
- Tools to cover tracks

Erase or Modify Evidence

System log files are the first place to check for questionable activity. Typically, hackers erase only the parts of the logs that show hacking actions. To the extent possible, a hacker makes the log appear as it did before the attack. This can be done without admin privileges. Hackers commonly delete the following logs in Windows files:

- SECEVENT.EVT logs failed logins and file access without privileges.
- SYSEVENT.EVT logs anomalies in system operations and driver failure.
- APPEVENT.EVT logs application variants.

These files are continuously open, running, and logging activity. A good hacker will remove any unnecessary files that were added during the hack and remove information in the files that were generated by the attack.

Hide Evidence

Another way to cover tracks is to hide the evidence. Following are methods a hacker can use to hide files.

- Choosing the hidden option in the file attributes menu will hide the file from directory listings and from browsing in Windows Explorer.
- Placing a period at the beginning of a Linux, Unix, and OS X file name hides the file.
- Placing the file in the unused or slack space of an existing file can hide a file. Because the file size was defined previously, there will be no indication that data was added to the file, and the data doesn't typically show up when opening the file.
- Incorporating the file in the ADS can hide it. ADS was created to allow compatibility with Macintosh files. One of its features is the ability to have multiple streams of data simultaneously. The alternate stream of data isn't seen in Windows Explorer.
- Using executables that can be activated from the command line, but will remain unseen. This allows the hacker to actively run programs undetected.

Modify Timestamps

Another method to cover tracks is to alter the timestamp on files. Each file gets stamped with a time and date each time it is created, accessed, or modified. You can use the following tools to do this:

Tool	Description
Timestomp	Timestomp is a tool for modifying or deleting a file's timestamp in order to hide when the file was created, accessed, or modified. Hackers change times and dates to blend in with existing timestamps so as to not alert digital forensic investigators of access or exploitation.
Touch	The touch command in Linux, Unix, and OSX can be used to alter the timestamp as well. It can change the time to the current time or to any specific time.
ctime	ctime is a header file that contains definitions of functions to get and manipulate date and time information.
Meterpreter	Meterpreter is Metasploit's payload. It has many features for covering tracks, including the ability to launch a fileless attack.

Disable Auditing

After gaining administrative access to a system, a hacker will typically install reconnaissance tools such as keyloggers to obtain logins and passwords. This action will be recorded in either the event login Windows or the syslog of Linux and other systems. These logs can be programmed to alert system administrators. To disable auditing, a hacker can use the Auditpol.exe command line utility to remotely change the audit security settings. AuditPol can be used to disable security auditing on either local or remote systems. It can also be used to enable auditing after the attack is over to avoid suspicion. A hacker can use Auditpol.exe to alter the audit criteria for categories of security procedures.

Cover Tracks

There are many ways to clear online tracks:

- Browse in private mode
- Delete history in address field and stored history
- Clear cookies and caches
- Delete downloads, saved sessions, and user JavaScript
- Disable the password manager and clear its data
- Create multiple users
- Clear Most Recently Used and toolbar data

There are additional tools available to help cover tracks:

Tool	Description
Ccleaner	Ccleaner is a cleaning tool that can remove files and clears internet browsing history. It also frees up hard disk space. It clears the temporary files, history, and cookies from each of the six major search engines.
Clear My History	Clear My History is software that can clear cookies, stored data like passwords, browser history, and temporary cached files. It can clear the recycling bin, clipboard data, and recent documents lists as well.
Dump event log	The dump event log command line tool in Windows 2000 dumps an event log remotely or on a local system into a tab-separated text file. It can also be used to filter specific types of events.