- Filename: eccouncil-ceh31250-v11-6-8-1-maintaining-access.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Maintaining Access
  ==

Maintaining Access

Objectives:

- Define Remote Application Execution
- List and describe tools and techniques used by attackers to remotely execute applications and maintain access to target systems
- Define NTFS Alternate Data Streams
- Explain how ADS can be used for malicious purposes
- Create and employ ADS
- Define rootkits and explain their goal
- List and define common rootkit types

- Application Execution
    - This is really the ability to interact with the target system
      after compromise
        - Run system commands
            - Remote Access Trojans
                - TheFatRat
                - Pupy
                    - Keylogging
                    - Screenshots
                    - Camera access
                    - Clipboard
            - Spyware
    - Defenses?
        - Anti-malware/AV
        - Anti-keylogger software
        - Anti-spyware software
        - Patches/Updates
- Alternate Data Streams
    - Used by attackers to hide malicious files
        - Attaches malware to legit files
            - Doesn't change size or properties of legit file
                - Create ADS
                    - `type malware.exe > C:\file1.txt:malware.exe`
- Rootkits
    - Malware that replaces OS files/processes with malicious versions
    - Standard backdoor capabilities
        - Command and Control

- Log wiping
- Monitoring
  -Types
- Boot-loader Level
  - Modify/replace boot loader with malicious copy
- Hardware/Firmware Level
  - Rootkit image is stored in firmware
- Kernel Level
  - Malicious code installed in the kernel
  - Highest level of OS access
- Hypervisor Level
  - Loads the target OS as a virtual machine
  - Intercepts and controls hardware calls to target OS
- Application Level
  - Like traditional malware
  - Runs as malicious versions of software and utilizes the original software's API calls
- Library Level
  - Hooks into high-level system calls