- Filename: eccouncil-ceh31250-v11-7-6-1-malware-analysis.md
- Show Name: CEHv11 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - Malware Threats
- Episode Name: Malware Analysis
  ==========

Malware Analysis

Objectives:

- Define sheep dipping
- Explain the basic malware analysis concepts, types, and procedures
- Identify common static and dynamic malware analysis techniques

---

- Basic details of Malware Analysis
    - Discovery, Study, and Reporting of malware and its attributes
        - Discovery
            - AV alerts
            - Monitoring
                - **Sheep Dipping**
                - Comes from Farming.
                - Sheep are treated as if they were infectious until they were disinfected
                - 'Cyber Sheep'
                - Computers, mobile devices, USB drives, email attachments, software, etc
                - Treated as infectious until...
                  + Scanned with AV(multiple)
                  + Monitored network activity
                  + Monitored processes
                  + Permissions checked
                  + Monitored Registry and Kernel
                  + Study
                  - What is this malware doing? *(aka 'reverse engineering')*
                  + Types of Analysis
                  1. **Static Analysis** (aka code analysis)
                  + File hashes
                  - Virus Total
                  - Hybrid Analysis
                  + Portable Executable(PE) Files
                  + Suspicious strings in code
                  + Obfuscations
                  + File dependencies
                  + Disassemble malware code
                  2. **Dynamic Analysis** (aka behavioral analysis)
                  + Disk/CPU/Memory/Network activity
                  - Create command and control channel
                  - Exfil data
                  - Destroy data
                  - DoS/DDoS
                  - Spying
                  - Testing Environment

+ Isolation is key
- Dedicated physical system
- Virtualization on dedicated system
+ Disable "shared folders" (**SHOW THIS IN VMWARE**)
+ Configure "Guest Isolation"
- Isolated network
+ VLAN
+ Firewall
+ Host-only
+ Install malware analysis tools
- Monitors
- Debuggers
- Report
+ Attributes are recorded
- IoC, Hash Values, sophistication level, exploited vulns, objectives, entry point
+ Signatures created
+ Alerts created
+ Attribution (if possible)
+ Lessons Learned