Infosys Class 2

15 February 2020 09:26

- S/w evaluation
  - A/v engine eval. : blacklist,greylist,whitelist
  - Sandbox analysis: A/v engine score, check droppers,dropper itself is agian sandboxed to evaluate; Cuckoo,limon,joe
  - Files created,deleted & modified
  - Registries
  - Outbound connection
  - Memory analysis
  - CVSS : Common vulnerability security score, vulnerabilities are tagged with CVE-ID
- Server hardening & Compliance
  - CIS/NIST/
  - Denying changing the root pswd
    - /sysroot
  - Password control
    - Service accounts: not assigned to any employees, but are required to
  - Idlesession timeout
  - Disabling ctrl+alt+del : it reboots the server in linux, disabling /usr/bin
  - Removing the default accounts: /sbin/nologin
  - Disabling the unused servers
  - DORA : DHCP Discovery Offer Request Acknowledgment
  - Denying root login
  - Permission for important files: set facl, umask, by default linux does give execute permissions
  - Firewall
  - MDT Imaging
  - Stealth rule
- DLP (Data loss prevention)
- Data loss policy
- Symantec dlp architecture