29 Feb Afternoon

29 February 2020 14:10

Infosys (Network + Data Security)

Software Evaluation
- AV Engine Evaluation
  - Blacklisted, Greylisted, Whitelisted
- Sandbox Analysis
  - Multiple VMs, job queue etc.
  - Evaluating Droppers (like temp files)
  - Files created, deleted, modified
  - Registries created, deleted, modified
  - Outbound connections
  - Memory Analysis
  - Examples: Cuckoo, Limon, Joe
- Checking the credits in reputed vulnerability databases
  - Common Vulnerability Security Score
    - CVE – ID - [Year]

Software Hardening / Compliance
- OS Hardening
  - Denying / Changing the root pass
  - Idle session timeout
  - Pass controls
  - Disabling ctrl + alt + delete
  - Removing default accounts
  - Disabling unused services
  - Denying root login
  - Permissions for imp files
  - Firewall
  - Securing ssh
  - Disabling usb
  - SE Linux evaluation
  - Privileged Identity/Access Management (Service Accounts)

- Setfacl – set access control list for each file
- Umask – default permissions

Ssh
- Latest protocols
- Login grace time
- Permit root login
- Idle session timeout
  - Client alive interval
    - Time duration
  - Client alive count max
    - Integer
  - Pings every client alive interval / count_max time to check if client is active
- Cipher MACs

Firewall
- Secure the appliance
  - DB
  - Customized Linux
  - Web console
  - Example: Checkpoint

- Restrict Logical Access
- Rules

1.

1. Stealth Rule	Malicious Files/ requests	Any Any Any Drop

2.

2. Web Console		IP IP http allow
3. ssh		IP IP ssh/22 Allow

3.

4. Cleanup	Others	Any Any Any Drop

DLP
-