PI-ADV

Windows 10 Image – list 1 on tools

Notes

Looks like a regular competition image

good README looks exactly like you would find in competition

a little creepy to be honest

README

* critical software
  + notepad++, firefox, filezilla client, ifranview
  + update to latest.
  + Bitlocker needs to be enabled. Full disk encryption need to be enabled.
* Critical services
  + openssh (ssh needs to operate on port 223)
  + file sharing smb (no hostage information on the server)

Forensic Quesitons

1. finding service name of the telnet server service.
2. Hidden network share, find who created the network share.
3. File with a phone number, what is the phone number of hostage arturo → 1-800-918-2102
4. who has full access on the network share → manila

if there is notepad++ check the history, there might be something there.

Windows firewall is disabled and cannot be turned on, at least I haven’t found a way yet.

LSP needs to be configured – lockout policy needs to be above 5 attempts

disable any shares that aren’t allowed.