TASK:

Recover – Ransomware

CONDITIONS:

Given a compromised machine infected with ransomware

STANDARDS:

1.) Team members disconnect machine from network to prevent ransomware spread

2.) Team members identify suspected ransomware files

3.) Team member obtain and compare a hash of the files and save them to a text file.

a. Hashes can be obtained at the command line using one of the tools referenced below and compared to previously known malware samples in the incident Indicators of Compromise (IOC).

b. Hashes can be obtained and verified automatically on VirusTotal using Windows GUI tools.

4.) Team members restore saved backup if one is available

5.) If a usable backup does not exist, team members remove suspected ransomware files and attempt to locate copies of files such as shadow copies or temporary files

END STATE:

Machine is recovered to most usable state available and suspected ransomware files are removed

NOTES:

1.) Tools: There are various Windows and Linux tools that can be used to obtain the hash. For example:

a. Md5deep / Hasheep - Linux or Windows

b. Md5sum / Sha1sum – Linux

c. Hfind - Linux

d. Sigcheck.exe – Sysinternals - Windows

REFERENCES:

https://christophergeiger3.github.io/UConn-x-National-Guard-Documentation/scenario2/

REVISION HISTORY:

19 APR 2021