Stuff from class

Christopher Adam Craig

In class today I mentioned several things that are worth posting:

1) It's not required for class, but every incident response person should watch the Shmoocon Wipe the Drive presentation: **https://www.youtube.com/watch?v=lb1XDMbQOiM** (https://www.youtube.com/watch?v=lb1XDMbQOiM)

▷

(https://www.youtube.com/watch?v=lb1XDMbQOiM)

2) The SANS Investigated Forensics Toolkit (SIFT) is a freely available VM that comes with a bunch of analysis tools. It's not a terrible start to putting together tools to run an investigation: **https://digital-forensics.sans.org/community/downloads** (https://digital-forensics.sans.org/community/downloads)

3) As you investigate, if you see logins from kyle or AD\kyle, please ignore them. They were the administrator and we know he isn't compromised. Also, if you see evidence the ssh server restarted we know that that was legitimate.

Search entries or author | Unread

Reply