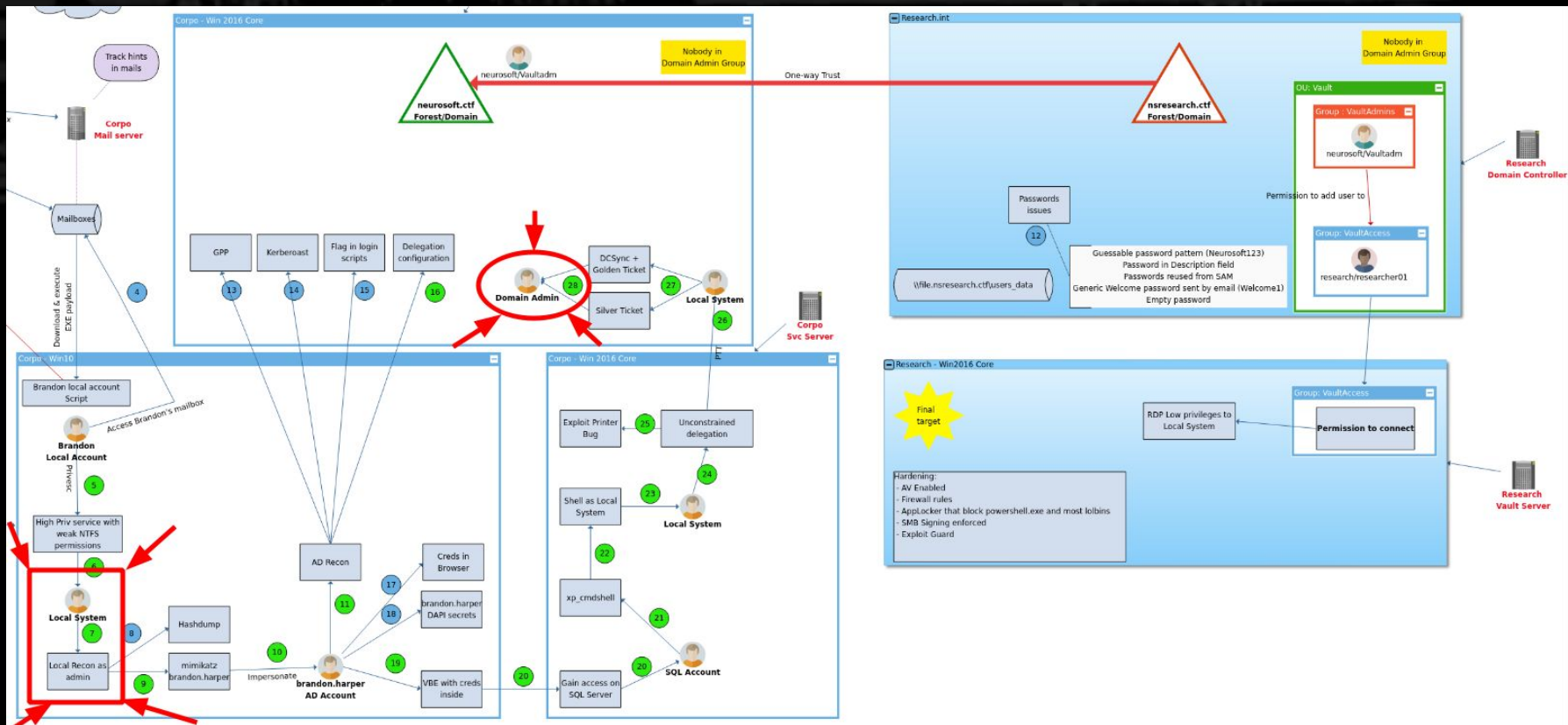




# NorthSec Windows Track

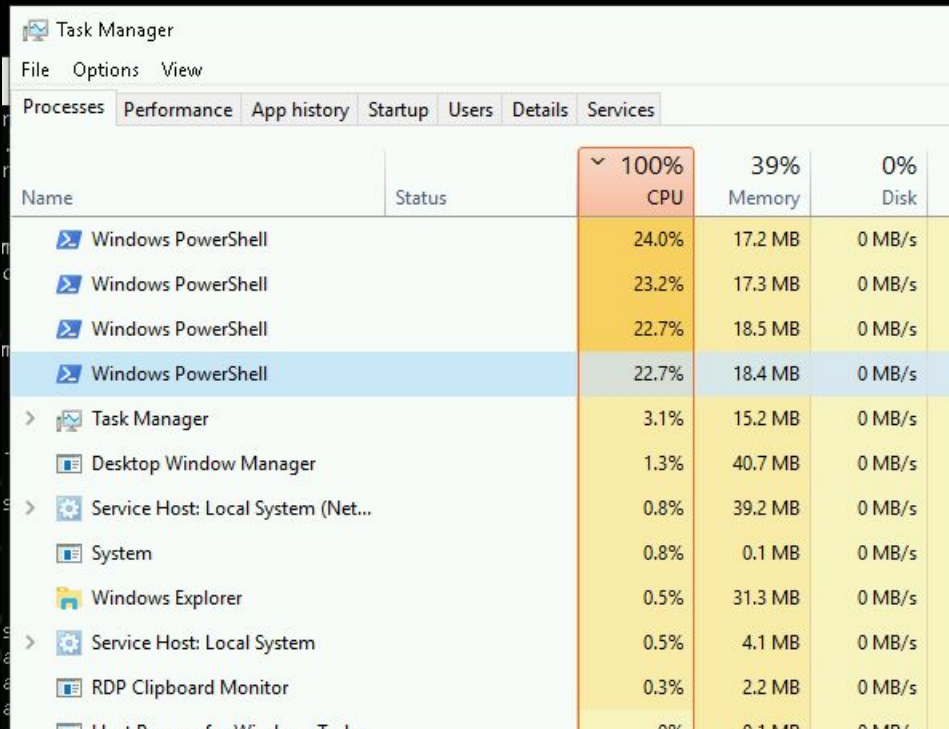
By Martin Dubé  
*Montréalhack - October 2019*

# Track Overview



# We will be sharing the same environment

- Avoid Migrate
  - Steal Tokens instead
- Avoid Spawning unnecessary processes
- Do not change passwords
- Do not delete files



The screenshot shows the Windows Task Manager application with the 'Performance' tab selected. The interface displays various system metrics. The 'Processes' tab is also visible in the background. The 'Performance' tab shows the following data:

Name	Status	CPU	Memory	Disk
Windows PowerShell		24.0%	17.2 MB	0 MB/s
Windows PowerShell		23.2%	17.3 MB	0 MB/s
Windows PowerShell		22.7%	18.5 MB	0 MB/s
Windows PowerShell		22.7%	18.4 MB	0 MB/s
Task Manager		3.1%	15.2 MB	0 MB/s
Desktop Window Manager		1.3%	40.7 MB	0 MB/s
Service Host: Local System (Net...)		0.8%	39.2 MB	0 MB/s
System		0.8%	0.1 MB	0 MB/s
Windows Explorer		0.5%	31.3 MB	0 MB/s
Service Host: Local System		0.5%	4.1 MB	0 MB/s
RDP Clipboard Monitor		0.3%	2.2 MB	0 MB/s
Host Process for Windows Tools		0%	0.1 MB	0 MB/s

# Helpers

## ➤ Tools

➤ C:\temp (DEV and SVC)

## ➤ Flags

➤ \\dc01.nsresearch.ctfusers\_data

# Your Mission: <https://bit.ly/2nLWz5W>

## ➤ Advanced users

- Get Domain Admin of Neurosoft.ctf
- Exploit Path
  - Host Recon; Look for a .VBE
  - Domain Recon; Impersonate first, then look for delegation setting
  - Get SYSTEM on SVC
  - Printer Bug -> Mimikatz/Rubeus
  - **OR** Bkp Share -> Silver Ticket
  - DA

## ➤ Beginners

- Find Passwords flags
  - alfred.lebrun, test.user, zim.armstrong, linda.costa, stuart.fagan, svcMoonCrackle