
# Windows API Exploitation Recipes for Red – Blue Teams

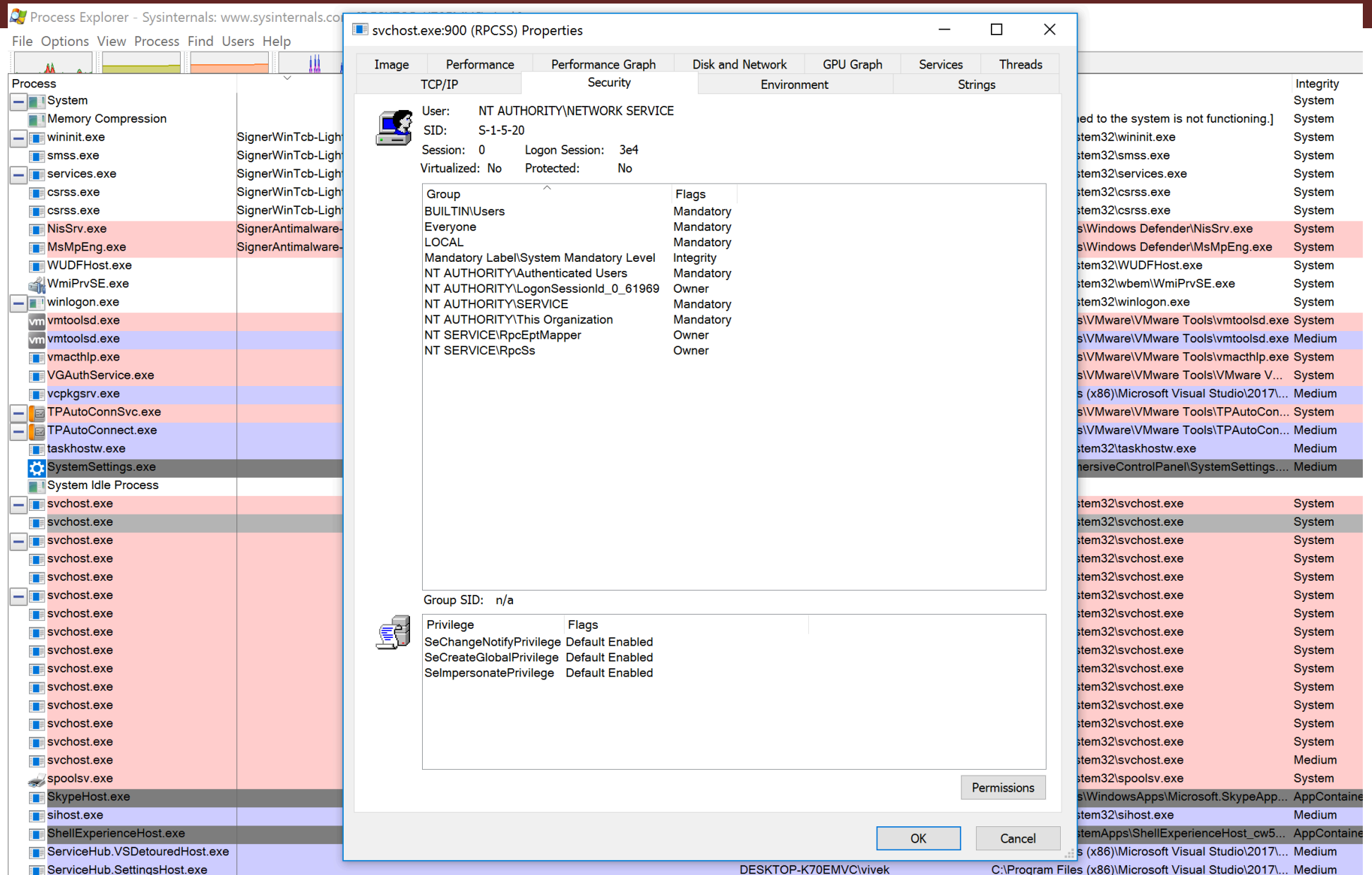
Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

# Process Token Dumper: Part 1
# The Basics

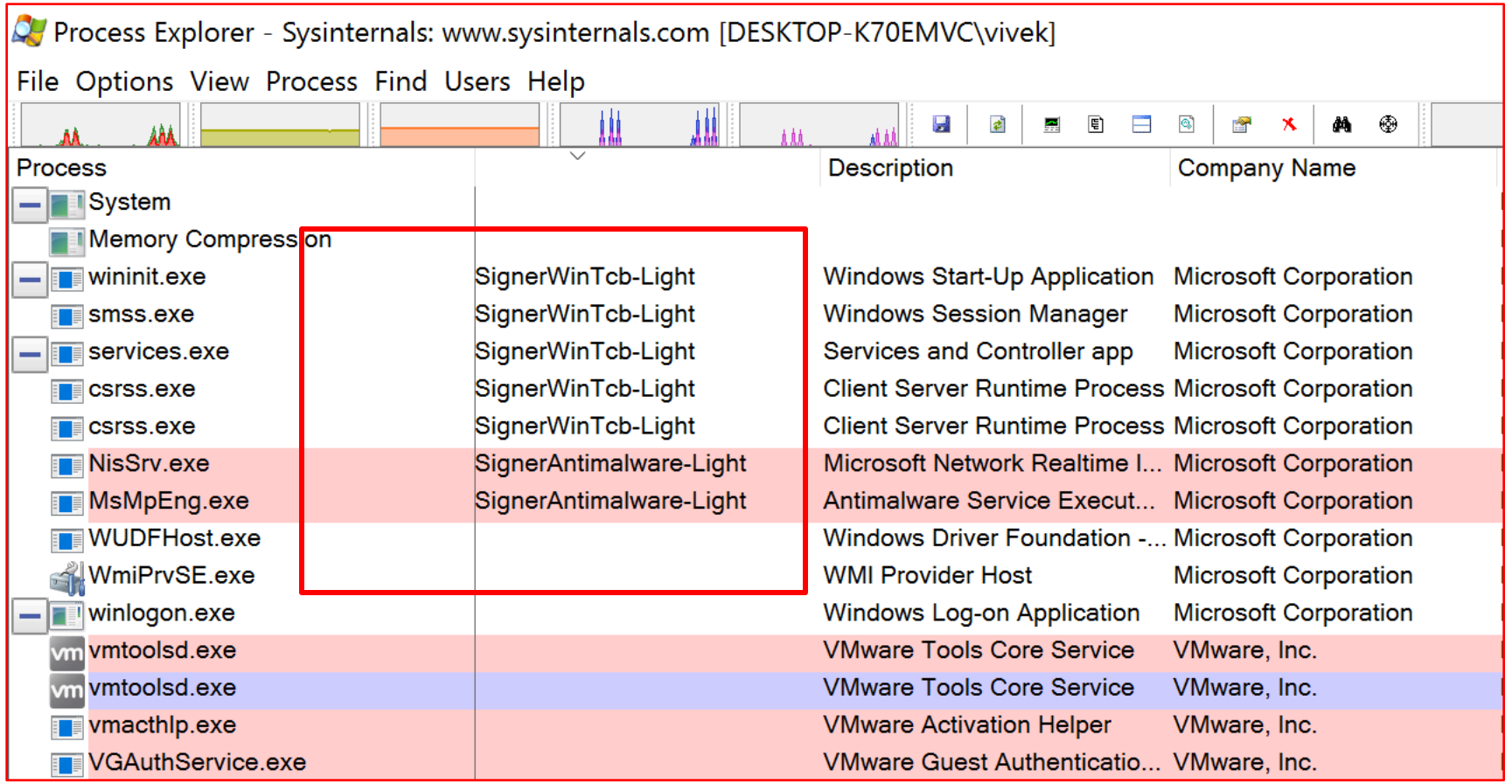
# What will you learn?



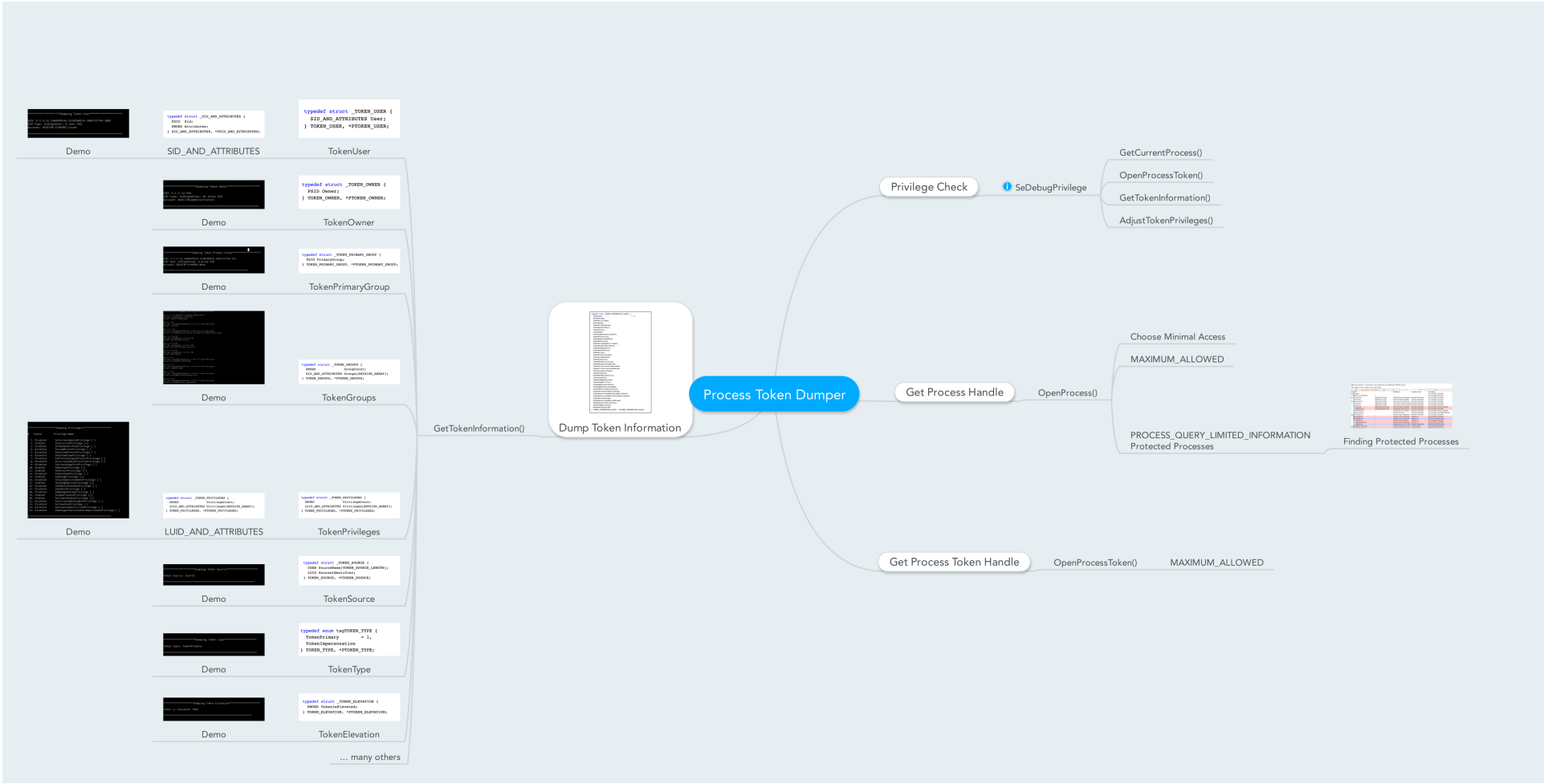
# What will you learn?

```
C:\Users\vivek\Documents\Visual Studio 2017\Projects\DumpProcessToken\Debug>DumpProcessToken.exe 788
[+] SeDebugPrivilege available for enabling![+] Enabled SeDebugPrivilege
Dumping token information for PID: 788

********************Dumping Privileges********************

#   Status        Privilege-Name

  1. Enabled       SeCreateTokenPrivilege [+]
  2. Disabled      SeAssignPrimaryTokenPrivilege [-]
  3. Enabled       SeLockMemoryPrivilege [+]
  4. Disabled      SeIncreaseQuotaPrivilege [-]
  5. Enabled       SeTcbPrivilege [+]
  6. Disabled      SeSecurityPrivilege [-]
  7. Disabled      SeTakeOwnershipPrivilege [-]
  8. Disabled      SeLoadDriverPrivilege [-]
  9. Enabled       SeSystemProfilePrivilege [+]
 10. Disabled      SeSystemtimePrivilege [-]
 11. Enabled       SeProfileSingleProcessPrivilege [+]
 12. Enabled       SeIncreaseBasePriorityPrivilege [+]
 13. Enabled       SeCreatePagefilePrivilege [+]
 14. Enabled       SeCreatePermanentPrivilege [+]
 15. Disabled      SeBackupPrivilege [-]
 16. Disabled      SeRestorePrivilege [-]
 17. Disabled      SeShutdownPrivilege [-]
 18. Enabled       SeDebugPrivilege [+]
 19. Enabled       SeAuditPrivilege [+]
 20. Disabled      SeSystemEnvironmentPrivilege [-]
 21. Enabled       SeChangeNotifyPrivilege [+]
 22. Disabled      SeUndockPrivilege [-]
 23. Disabled      SeManageVolumePrivilege [-]
 24. Enabled       SeImpersonatePrivilege [+]
 25. Enabled       SeCreateGlobalPrivilege [+]
 26. Disabled      SeTrustedCredManAccessPrivilege [-]
 27. Disabled      SeRelabelPrivilege [-]
 28. Enabled       SeIncreaseWorkingSetPrivilege [+]
 29. Enabled       SeTimeZonePrivilege [+]
 30. Enabled       SeCreateSymbolicLinkPrivilege [+]
 31. Enabled       SeDelegateSessionUserImpersonatePrivilege [+]

*******************************************************


C:\Users\vivek\Documents\Visual Studio 2017\Projects\DumpProcessToken\Debug>
```

# What will you learn?



# Token Dumper MindMap



# Thank You!