Windows Secure Script Flow

1. Sets variable for ccdc path
2. Sets user input for OS as variable 'box'
3. Checks for admin permissions (branches for new vs. old)
4. Sets variables for hardcoded IPs in competition (for use in firewall rules)
5. Requires input to make sure IPs are right
6. Sets variable for Domain Name (for use in login banner)
7. Finally makes ccdc directory, Registry Backup directory, and SMBProof directory
8. Copies %systemroot%\system32\drivers\etc\hosts to ccdc\hosts
9. Pauses
10. Exports old firewall to ccdc\firewall.old
11. Enables logging for firewall
12. Braches for firewall rules and registry
13. Configures general firewall rules, login banner
14. Makes file ccdc\regproof.txt to record changes to registry (Notes before each section)
15. REG: queries owner, changes registered owner to blueteam, queries again
16. REG: queries for image hijack that kills Taskmanager, then deletes it
17. REG: queries for policy that disables Taskmanager, then deletes it
18. REG: queries for policy that disables CMD, then deletes it
19. REG: queries for hiddenfiles, changes, queries again
20. REG: queries for superhiddenfiles (system), changes , queries again
21. Fixes Local Security Authority by:
22. REG: queries for restrictanonymous, changes , queries again
23. REG: queries restrictanonymoussam, changes , queries again
24. REG: queries everyoneincludesanonymous, changes , queries again
25. REG: queries for enableplaintextpassword, changes , queries again
26. REG: queries for nolmhash, changes , queries again
27. REG: queries usemachineid, deletes it
28. REG: queries notification packages, changes , queries again
29. REG: queries specialaccounts, deletes it
30. Goes to specific box, configs specific firewall rules
31. SMBv1 fix!!!! Uses powershell to save previous SMB1 config to ccdc\SmbProof\SMBDetect.txt, changes and appends to it.
32. Configs NTP server for Win 8+
33. Export registry:
34. REG: export HKLM %ccdcpath%\Regback\hlkm.reg
35. REG: export HKCU %ccdcpath%\Regback\hkcu.reg
36. REG: export HKCR %ccdcpath%\Regback\hlcr.reg
37. REG: export HKU %ccdcpath%\Regback\hlku.reg
38. REG: export HKCC %ccdcpath%\Regback\hlcc.reg
39. End