# CYB394 – Windows Security Lab 1

# Part 1

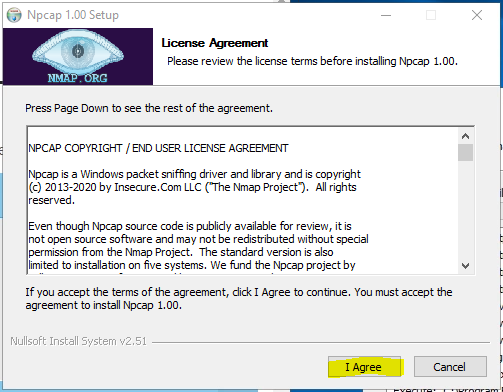
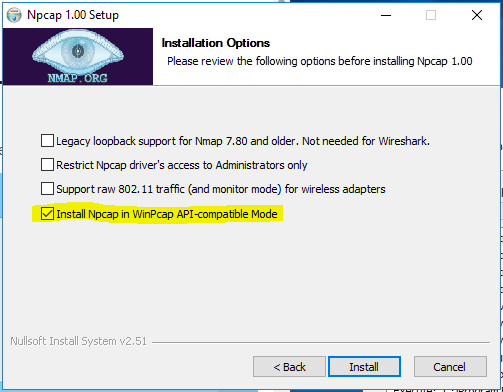
1. **Sign-In to SRV1 as Administrator (Password1)**
2. **Set Administrator account password properties:**  
   Server Manager -> Tools -> Computer Management -> Local Users & Groups -> Users -> Administrator -> Set the built-in **Administrator Password never expires.**
3. **Set Server IP Address:**  
   Server Manager -> Local Server -> Ethernet0 -> click ‘IPv4 address…’  
   The server is part of the 10.0.0.0/24.  
   Set the following IP address information

IP v4 Address 10.0.0.10

Netmask Decimal form of /24

Gateway 10.0.0.254

Preferred DNS 8.8.8.8

1. When prompted for **Network Discovery click [Yes]**
2. **Change Server Name:**  
   Server Manager -> Local Server -> click ‘Computer Name’ -> [Change] -> Set the name of the computer to be SRV1  
   **Reboot server when prompted.**
3. **Sign-In into SRV1 as Administrator (Password1)**
4. **Pin File Manager to Taskbar**
5. **Launch IE** from the taskbar (Don’t use recommended settings & Do Not Send Tracking) and **install Google Chrome.**
6. **Google “Install Wireshark” -> Download & install Wireshark(64) &Npcap**  
     
   ~~  
     
   Finish Wireshark install with defaults and Reboot when Prompted.
7. **Unpin IE from Taskbar**
8. **Pin Chrome to Taskbar**
9. **Install the Active Directory Domain Services (ADDS) role**  
   Server Manager -> Dashboard -> Add roles and features -> Active Directory Domain Services -> Install with Defaults.
10. **Promote SRV1 to (\*) Add a New Forest** domain controller as **CYB394XX.PRI (XX are your initials, eg: CYB394JS.PRI John Smith)**  
    Be sure to allow DNS to be installed and configured during the promotion process. When prompted for DSRM password use **Password1  
    Prerequisites Check may have warnings but will [Install]  
    Reboot when complete.**
11. After Domain install Sign-In as Administrator (Password1).
12. **Verify Administrator account to Domain Admins, Enterprise Admins and Schema Admins groups:**  
    Server Manager -> Tools -> ADUC -> Users -> Administrator -> Properties -> Membership -> [Add] Domain admins, Enterprise admins & schema admins

|  |
| --- |
| Screenshot of Administrator -> Properties -> [Member of] tab |

1. Create a new Personal Domain Administrator (PDA) account with your first name, last name and set a logon name as first initial, last name (eg: JSmith).
2. Set the password to **Password16** and set Password Never Expires. Add this user to the Domain Admins, Enterprise Admins & Schema Admins security groups

|  |
| --- |
| Screenshot of PDA -> Properties -> [Member of] tab |

1. Sign-Out then Sign-On with your personal domain admin account
2. Open DNS using the DNS tool and verify forwarder to 8.8.8.8. (dns.google)

|  |
| --- |
| Screenshot of SRV1 DNS Properties -> [Forwarders] tab |

1. Create a reverse lookup zone for the domain in the 10.0.0 network address using defaults.

|  |
| --- |
| Screenshot DNS -> Reverse Lookup zone for CYB394XX.PRI |

# Part 2

1. **Sign-In to SRV2 as Administrator (Password1)**
2. Set IP address settings so that you can join SRV2 to CYB394XX.PRI  
   IP v4 Address **10.0.0.20**

Netmask Decimal form of /24 (255.255.255.0)

Gateway 10.0.0.254

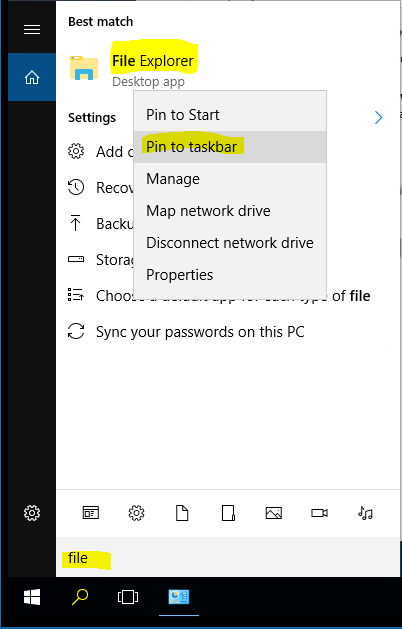
Preferred DNS **IP address of SRV1**

1. Change name of the computer to **SRV2 -> Reboot**
2. **Join SRV2 to the CYB394XX.PRI** domain using your PDA as authentication -> **Reboot**.
3. Sign-On to SRV2 with your **PDA** account (**Password16**)
4. Verify internet connectivity
5. Launch IE -> Install Chrome & Wireshark
6. Unpin IE from Taskbar
7. Pin Chrome to Taskbar
8. Verify that SRV2 has a registered forward and reverse lookup address in DNS (SRV1)

# Part 3

1. ***Sign-On to SRV3 with your PDA account (Password16)***
2. Repeat the same processes for the virtual machine labeled SRV3.
3. Change IP address to 10.0.0.30
4. **Change the Server name to SRV3 -> Reboot**
5. Join SRV3 to the CYB394XX.PRI domain
6. Sign-On to SRV3 with PDA (Password16)
7. Install Chrome & Wireshark
8. Unpin IE from Taskbar
9. Pin Chrome to Taskbar

# Part 4

1. Sign-On to CLIENT1 with the **Student** account (**Password10**)
2. Repeat the same process for the virtual machine labeled CLIENT1.
3. Change IP address to 10.0.0.50
4. **Change the machine name to CLIENT1 -> Reboot**
5. Join CLIENT1 to the CYB394XX.PRI domain
6. Sign-On with PDA (Password16)
7. Install Chrome & Wireshark
8. Pin Chrome to Taskbar
9. Pin File Explorer to Taskbar  
   

# Part 5: Configure SRV1 to use an External Time Source

1. Sign-In to SRV1 with PDA and issue the following command from an **elevated command prompt**, type on a single line.

w32tm /config /manualpeerlist:"tick.usno.navy.mil" /syncfromflags:manual /reliable:yes /update

1. To check that these were set, use the following command.

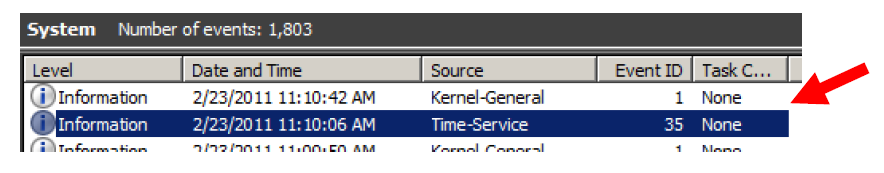
w32tm /query /peers

|  |
| --- |
| Screenshot of w32tm /query /peers command: |

1. To resync with time sources, issue this command

w32tm /resync

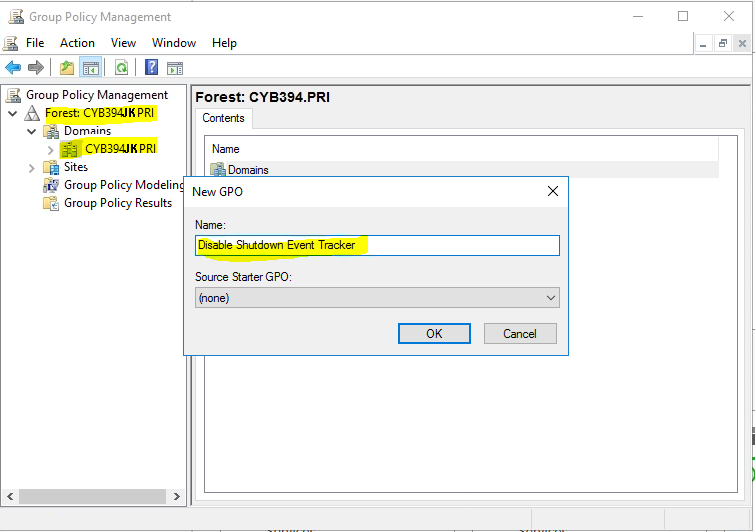
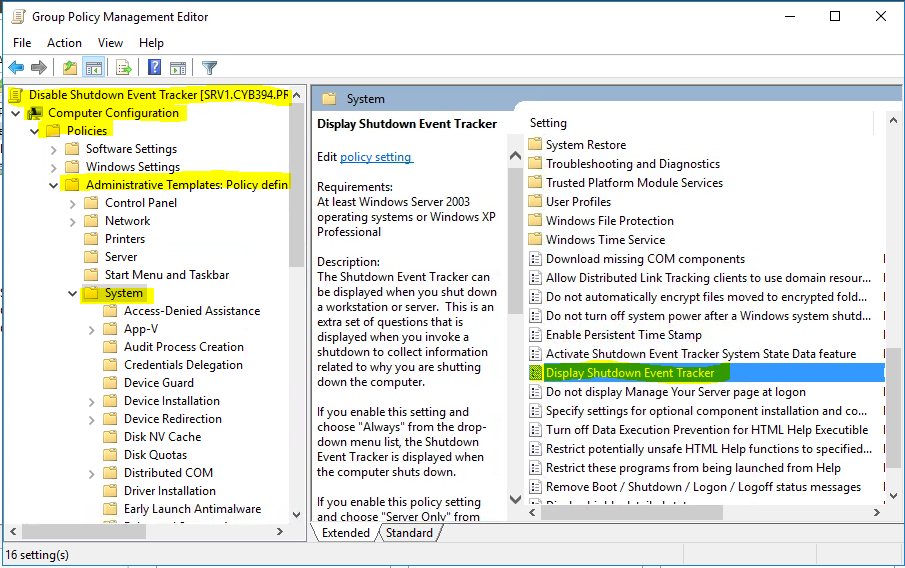
1. Check the Event Viewer and look in the Windows System log for Events ~~1~~ & 35.



# Part 6

1. **Sign-In to SRV1 with your PDA. (Password16)**  
   ~~(Your other images should not be running yet.)~~

To make lab work easier **stop displaying the Shutdown Event Tracker** when you shut down or restart.

1. Create a new Group Policy Object called **Disable Shutdown Event Tracker and link the policy to the CYB394XX.PRI Domain** container. While you shouldn’t disable the Shutdown Event Tracker in a production environment, it helps to do this in a lab or testing situation.  
   
2. The policy setting is in the Computer Configuration -> Policies -> Administrative Templates -> System folder. Locate the *Display Shutdown Event Tracker* policy and Disable  
   
3. Configure the policy so that the Shutdown Event Tracker will not be displayed.
4. Open an elevated command prompt and force the new policy to be applied to your computer. (gpupdate /force)
5. Run GPRESULT /R to verify that the new policy is being applied.

|  |
| --- |
| Screenshot of CMD -> gpupdate /r command -> Computer Settings: |

1. Restart SRV1.

# Part 7 Password Policies

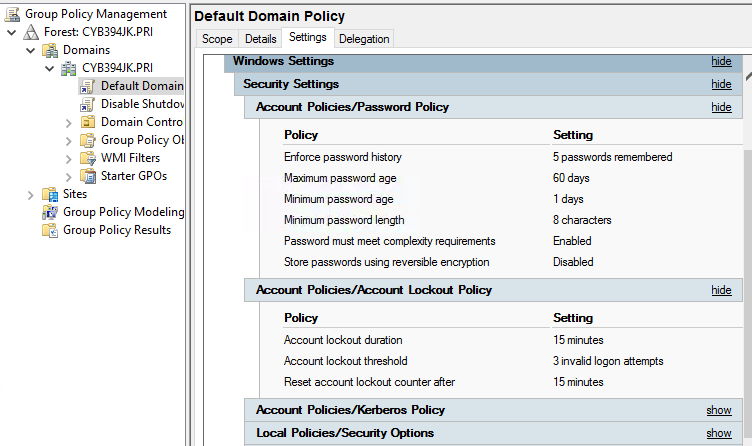
1. Sign-In to SRV1 with your PDA.

Modify Password Policies:

1. Server Manager -> Tools -> Group Policy Management -> **CYB394XX.PRI and Edit the Default Domain Policy** -> Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Password Policies/Account Policies
2. Adjust the Account Policies to accomplish the following objectives.

* Password Policies
  + Passwords to be at least **8 characters** in length
  + Users must change passwords at least once every two months (**60 days**).
  + The system is to **remember the last 5 passwords** each user has used and don’t want any of those to be reused.
  + A user must wait at least **two days** before changing a password once it has been changed.
  + Pass phrases should be complex.
  + Incorrect password attempts should force a lockout of 5 minutes.
* Account Policies:
  + 3 bad password attempts are allowed before lockout.
  + Account lockout duration is 15 minutes

**Close the Group Policy Management Editor**

**Refresh the Group Policy Management console and display the new Default Domain Policy settings**

|  |
| --- |
| Screenshot of Account Policies / Password Policy & Account Lockout Policy settings (ensure your full domain name is displayed): |

# Part 8

1. Sign-In to SRV1 with your PDA
2. Server Manager -> Tools -> ADUC -> Create a new OU called **CYB394** within the CYB394XX.PRI domain container.

|  |
| --- |
| Screenshot of ADUC showing full hierarchy: |