Windows CCDC:

# Turn on windows firewall:

* + Run > **gpmc.msc** > Forest > Domains > Find where the computers users are stored > right click where computers are stored ? click create a GPO in this domain, and link it here… > name it > press ok > right click edit > go to Computer config > policies > Windows Settings > security settings > windows defender firewall with advanced security > right click Windows defender firewall > edit polices > turn on firewall and block inbound and outbound connections > go to each tab and repeat previous step > save >
  + Check inbound and outbound rules to make sure there are no stupid rules
  + For containers = **Get-ADComputer –filter \* -Searchbase "cn=computers, dc=Contoso,dc=com" | foreach{ Invoke-GPUpdate –computer $.name -force}**
  + For OU’s = **Get-ADComputer –filter \* -Searchbase "ou=Accounting, dc=Contoso,dc=com" | foreach{ Invoke-GPUpdate –computer $.name -force}**
  + Locally = **Invoke-gpupdate –force**

# Account Management:

* Changing everyones domain passwords at once
  + **Get-ADUser -Filter \* | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText “PASSWORD” -Force)**
* Changing a users password at once
  + **gwmi -class win32useraccount -filter localaccount=true | % {net user $.name “PASSWORD”}**
* Disable unneeded user accounts
* **Change Admin Account passwds manually to something different then the rest of users.**
* Make sure accounts are in the correct groups(groups are in a container cn=Users)
  + Check Domain Admins, Schema Admins, and Enterprise Admins
* Rename built-in admin accounts on non-DC’s
  + Search lusrmgr.msc

# Check File Sharing Permissions

* + If there is a shared folder we need to make sure the access to it isn’t applied to non-admin accounts.
  + If there isn’t one lets create one now:
    - Go to your “C:” drive and make a new folder called “SharedFolder”
  + Right-click and shared folder and click ‘Properties’’
  + Click “Share”
  + Now add any users that need access, or remove users who do not need access
  + Here you can also add groups like Domain Admin, Enterprise Admins, Schema Admins.
    - This will affect any user attached to that group

# Install Firewall and defense software

* + Install a firewall if there is none.
  + Enable Windows Defender, download MalwareBytes
    - <http://bit.ly/2HSL7NB>
  + Get Comodo KillSwitch
    - <http://bit.ly/2FAyftZ>

# Check External facing services

### Web Service

* + Check in C-drive for folder called “inetpub”
  + Make sure you have a backup
  + Look through the code for anything malicious.

### Connections – We need to make sure there is no NC listners or SMB shares that do not need to be on here.

* + For this run ‘**netstat -a**’ in cmd
  + If installing applications is allowed just run **Comodo KillSwitch**

# Make Backups of all critical services

### Backup DNS Zone

* Open DNS Manager on the DC as this is usually where the DNS server is hosted
* Here look in fwd/rev lookup zone folders, these are the zones to backup.
* Now open CMD and run:
  + **dnscmd zonename /zoneexport Zone.com backup\zone1.com.dns.bak**
  + **Export-DnsServerZone -Name \_msdcs.ccdc.lan -FileName \_msdcs.ccdc.lan.bkp**
* Now you can go to **C:\Windows\System32\dns\backup\zone1.com.dns.bak** and use the backup to restore dns in the future(if needed)

# Check Startup Programs

If Comodo KillSwitch is installed use it to check these.

### Check for Sus Startup programs

* Or type ‘msconfig’ in run
* Or open task manager (taskmgr)

### Check for Scheduled Tasks

Red teams are known for using scheduled tasks to establish persistence, like have a payload run everytime you log on or every five min. This should be checked thoroughly.

* Launch Run, type **taskschd.msc** and then press enter on your keyboard
* Once here you can sift through the hundreds of folders or you can click “Task Scheduler(Local)” to see if there are and scheduled scripts that look malicious if there are some, delete them.

# Patch Critical Vulnerabilities

* For XP, 2000 and 2003 patch MS08\_067
* For Vista and 2008 patch MS09\_050
* For Windows Server 2012,2016, Windows 7,8,10 patch Eternal Blue and BlueKeep

# Set Policies – Active Directory – Add Group Policy Object MMC

### Password Policy

* Open “Run” and type **gpmc.msc** to open Group Policy Management Center.
* Edit the “Default Domain Policy” or and policy that is over all domain OUs in GPMC
* Navigate to ComputerConfig > Policies > WindowsSettings > SecuritySettings > AccountPolicy > **PasswordPolicy**
  + Min Pwd Length – 14
  + Enforce Pwd History – 3
  + Pwd Complexity – Enabled

### Disable storing passwords with reversible encryption

### Disable script execution

49:00 YouTube

# Download tools (and place them in a shared folder)

# Remove Unwanted Viruses and Software

# Patch at the very end!