Windows 10 Playbook

Install EDR / AV / Tools

Enable All Defender Tenants **(Turn tamper protection on in GUI)**

```
:defend
```

```
Set-MpPreference -DisableRealtimeMonitoring $false; Set-MpPrefer
```

Enable windows firewall

```
:firewall
```

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled T
```

Enumerate local administrators

```
:localadmin
```

```
Get-LocalGroupMember -Group "Administrators" | Select-Object Nam
```

Enumerate local users

```
:localuser
```

```
Get-LocalUser | Select-Object Name
```

Download hardening scripts

```
:scripts
```

```
$url = "https://github.com/gerbsec/cyberherd-scripts/archive/re
```

**** INSTALL HERDWAREBYTES IF DEFENDER IS BROKEN ****

MODIFY THE FOLLOWING SCRIPTS TO INCLUDE THE ACCT YOUR ARE LOGGED IN TO

```
removeUsers.ps1 and 2-passwordandsshlocalusers.ps1
```

Remove users not on the provided list (MODIFY THE LIST TO EXCLUDE YOUR ACCT)

```
.\removeUsers.ps1
```

Change all local user passwords not in array (MODIFY TO INCLUDE YOUR ACCT)

```
.\2-passwordandsshlocalusers.ps1
```

Download & unzip Sysinternals Suite & make C:\tools + Launch ProcExp,TCPView,ProcMon

```
:sysint
```

```
New-Item -ItemType Directory -Path 'C:\tools\' -Force ; $Progre
```

Run OS hardening batch script

```
hardenOS.bat
```

Run OS hardening PowerShell script

```
.\Hard.ps1
```

Enable event auditing

```
.\auditingOn.ps1
```

```
:cmdlog
```

```
New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerS
```

Download Sysmon Config & Run sysmon

```
:sysmon
```

```
$ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -Uri
```

Check Services.msc for suspicious services

```
Launch services.msc as Administrator
```

Monitor for new services

```
.\ServiceMonitor.ps1
```

Make sure no other users other than yourself are under allowed user accounts for RDP

```
Search remote desktop -> RDP settings -> Select users that can
```

Check current user sessions

```
Query session
Query user
```

Check open ports

```
:openports
```

```
netstat -aon | findstr LISTENING
```

Open Event Viewer, monitor SysMon events

```
Sysmon logs in Applications and Services -> Microsoft -> Windows
```

Manually audit task scheduler for suspicious tasks

(FOR THE END OF PLAYBOOK) Block all ports but IF WE CAN

```
:firewallall
```

```
New-NetFirewallRule -DisplayName "Deny All Except SSH and RDP" -
```