🧩 Microsoft Edge Baseline Hardening (Windows 11)

🔒 Overview

This project automates and verifies the **Microsoft Edge Security Baseline** on Windows 11.

It applies Microsoft's recommended browser security policies through scripts, checks if they are written to the registry, and confirms they are enforced inside Edge.

⚙️ What This Does

1. Applies Microsoft Edge baseline policies automatically using `Edge_Baseline_SelfSetup.cmd`

2. Saves proof that those policies are active inside Windows and Edge

3. Allows rollback with `Edge_Baseline_SelfRemove.cmd`

4. Uses only official Microsoft tools and built-in Windows features

---

🧰 Tools Used

- **LGPO.exe** → applies local Group Policy settings

- **Policy Analyzer** → verifies registry-level policies

- **Edge ADMX Templates (v139)** → defines the baseline

- **PowerShell / CMD** → automation scripting

🧱 Project Folder Layout

```
Edge-Baseline-Hardening/
 |
 ├— Edge_Baseline_SelfSetup.cmd ← apply policies
 ├— Edge_Baseline_SelfRemove.cmd ← remove policies
 |
 ├— Evidence/
 |  ├— EdgeBaseline_Clean_PolicyRules.xml ← baseline blueprint
 |  ├— Edge_Policy_Verification.json ← browser verification
 |  └— README_Evidence.txt
 |
 ├— Proofs/
 |  ├— PolicyAnalyzer_View.png ← registry proof
 |  ├— Edge_Mandatory_OK.png ← browser proof
 |  └— README_Proofs.txt
 |
 └— Microsoft-Tools/
 ├— LGPO.exe
 ├— PolicyAnalyzer/
 └— Microsoft Edge v139 Security Baseline/
```

yaml

Copy code

🧩 Registry Snapshot

After running the setup, the following keys are created under

`HKLM\SOFTWARE\Policies\Microsoft\Edge`:

Policy	Value	Purpose
SmartScreenEnabled	1	Enable SmartScreen protection
PreventSmartScreenPromptOverride	1	Block bypass of SmartScreen warnings
TypoSquattingCheckerEnabled	1	Detect fake/malicious URLs
ApplicationBoundEncryptionEnabled	1	Encrypt app-bound data
HttpsOnlyMode	1	Enforce HTTPS-only browsing

🔍 Verification Steps

Step	Tool	Result
1️⃣ Baseline	Policy Analyzer (.xml)	Blueprint of security settings
2️⃣ Registry	Policy Analyzer View	Shows applied policies in registry
3️⃣ Browser	Edge (`edge://policy`)	Confirms policies are active ("Mandatory OK")

📄 Results

- ✅ Policies successfully applied to Windows registry

- ✅ Verified in Edge browser (`edge://policy`)

- ✅ Full rollback supported

- ✅ Evidence and screenshots included

⚠️ Note

For **testing and security lab** use only.

Run as **Administrator** on Windows 10/11.

Scripts use only official Microsoft tools — no third-party code.