Topic no 67: A Look At DISA STIGs (2)

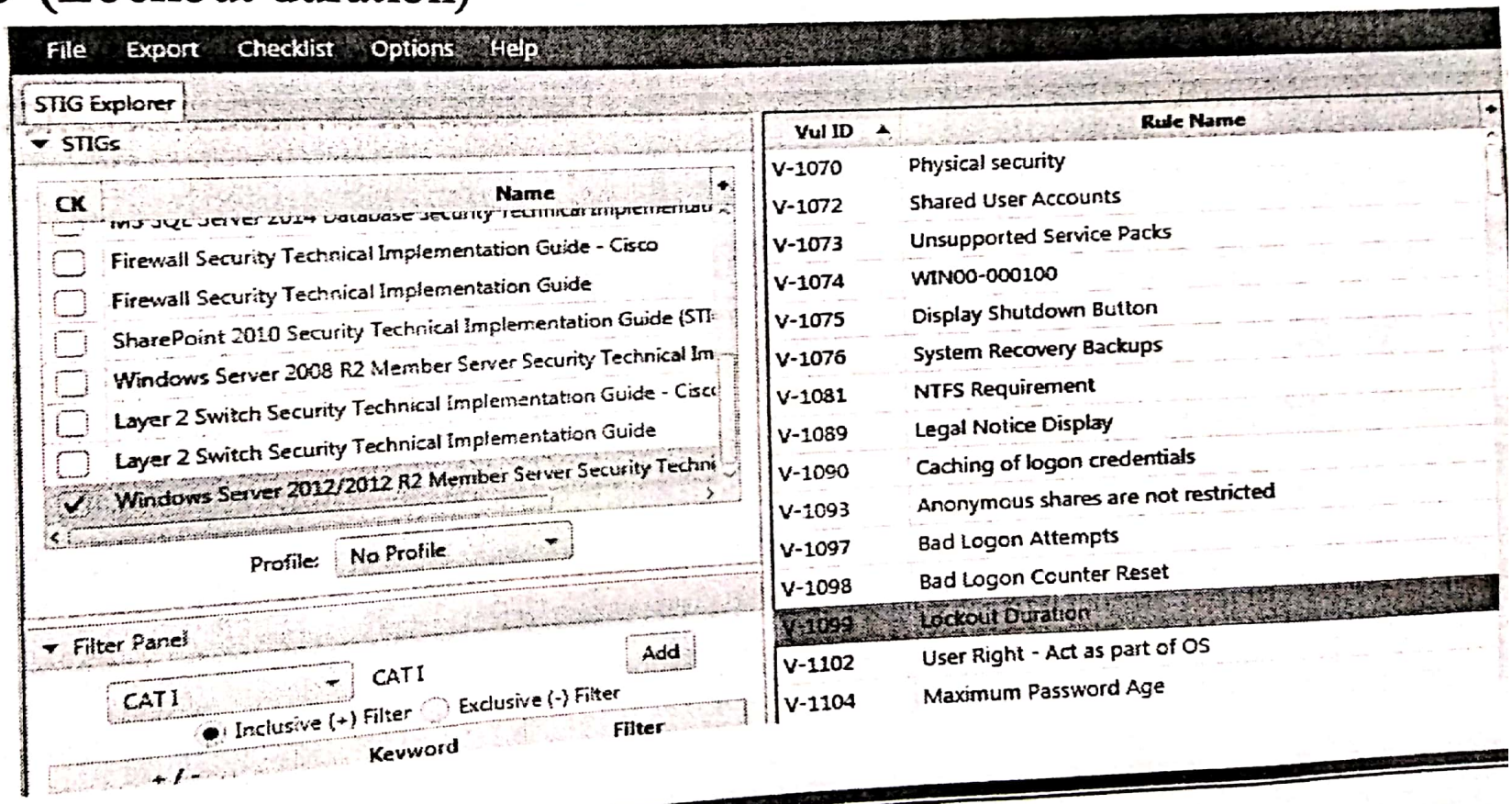
STIG content:

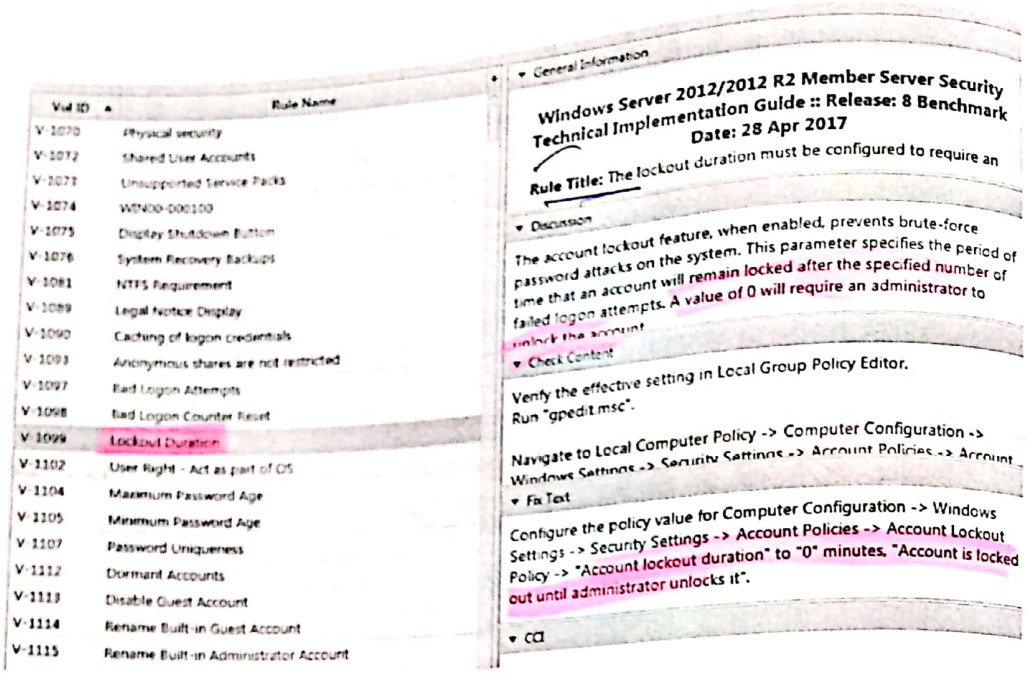
- General information (title)
- Discussion
- Check content
- Fix text
- CCI (References)

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

Topic no 68: A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
  - Import STIG
  - V1099 (Lockout duration)





Vul ID	Rule Name
V-1070	Physical security
V-1072	Shared User Accounts
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1075	Display Shutdown Button
V-1076	System Recovery Backups
V-1081	NTFS Requirement
V-1089	Legal Notice Display
V-1090	Caching of logon credentials
V-1093	Anonymous shares are not restricted
V-1097	Bad Logon Attempts
V-1098	Bad Logon Counter Reset
V-1099	Lockout Duration
V-1102	User Right - Act as part of OS
V-1104	Maximum Password Age
V-1105	Minimum Password Age
V-1107	Password Uniqueness
V-1112	Dormant Accounts
V-1113	Disable Guest Account
V-1114	Rename Built-in Guest Account
V-1115	Rename Built-in Administrator Account

General Information

Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide :: Release: 8 Benchmark Date: 28 Apr 2017

Rule Title: The lockout duration must be configured to require an

Discussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.

Check Content

Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account

Fix Text

Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes. "Account is locked out until administrator unlocks it".

CCI

- **Rule Title:**
  - The lockout duration must be configured to require an administrator to unlock an account
  - Severity: CAT II
- **Discussion:**
  - The account lockout feature, when enabled, prevents brute-force password attacks on the sys This parameter specifies the period of time that an account will remain locked after the speci number of failed logon attempts. A value of 0 will require an administrator to unlock account.
- **Check Content:** For MCQs.
  - Verify the effective setting in Local Group Policy Edi Run "gpedit.msc".
  - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Secu Settings -> Account Policies -> Account Lockout Policy.
  - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock account, this is a finding.
- **Fix Text:**
  - Configure the policy value for Computer Configuration -> Windows Settings -> Secu Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to minutes
  - "Account is locked out until administrator unlocks it".
  - CCI: NIST SP 800-53 Revision 4 :: AC-7 b

Topic no 70: Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

Diff b/w CIS & DISA

FEATURE	CIS	DISA
(1) CONTROL COVERAGE	GOOD	EXCELLENT
(2) ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
(3) USER FRIENDLINESS	GOOD	SATISFACTORY
(4) UNUSABLE TERMINOLOGY	NO	YES
(5) CONTROL DETAIL	GOOD	SATISFACTORY
(6) TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)
(7) CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
(8) TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
(9) FREQUENCY OF UPDATES	FAIR	QUARTERLY
(10) INDUSTRY CREDIBILITY	HIGH	VERY HIGH
(11) INDUSTRY ADOPTION	HIGH	MODERATE

How to select CIS/DISA: