

Topic No 1: What is Information Security?

- [REDACTED]
- IT Security
- Information security [REDACTED]
- IT Security functions:
 -
 -
 -
 -
- InfoSec functions:
 -
 -
 -
 -
- What is Cyber Security?
 - [REDACTED]
 -
- [REDACTED]
 - Confidentiality
 - Integrity
 - Availability:

Topic No 02: Why Is Information Security Needed?

- **Bangladesh Bank SWIFT Hack – Feb 2016:**

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- **The Importance Of Information**

-

- [REDACTED]
- [REDACTED]
- [REDACTED]

Topic No 03: Who Is Information Security For?

- **Personal:**

-
-
-
-

- **Organizational:**

-
-
-

- **Govt and national:**

-
-

—
—
—
—
—

-
-
-
-
-

-
-
-

Topic No 04: How Is Information Security Implemented?

- **Three pillars of information security:**

-

-

-

- **Leadership commitment:**

-

-

-

-

-

-

- **Information Security Manager or CISO:**

-

- **IT user:**

-

-

-

-

-

-

-

- **Business user:**

-

-

-

-
-
- **Information security program**

-
-
-
-

Topic No 05: Who Are The Players In Information Security?

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- **Government:**

-
-
-
-
-
-

- **Industry & sectors:**

-
-
-
-

-

-

- **International organizations:**

-

-

-

- **Professional associations:**

-

-

-

-

-

- **Academia & research organizations:**

-

-

-

Topic No 06: Infosec Transformation Framework 4 Layers

1: Security hardening:

-

-

-

-

-
-

2: Vulnerability management:

-
-
-
-
-

3: Security engineering:

-
-
-
-
-

4: Security governance:

-
-
-
-
-

Topic No 07: What Is Information Security Hardening?

- **IT assets**
- **Security hardening**

- **Security in the “trenches:”**

-
-
-

- **Why is security hardening at the first step in the security transformation model?**

-

-

- **Short example of Cisco router security hardening:**

-

-

-

Topic No 08: What Is Information Security Governance?

-

-

- **IT Governance Institute Definition:**

[Redacted]

- **ISO27001:2013 – ISMS** (Information Security Management System)

- **ISO27001** [Redacted]

- [Redacted]

- [Redacted]

Topic No 09: Difference Between Policy, SOP, & Guideline

- **Policy:**

– [Redacted]

- **Policy:**

–

– [Redacted]

- **Procedure / SOP:**

– [Redacted]

–

–

- **Guideline:**

- [redacted]
-
-

- **Standard:**

- [redacted]
-
-

- **In practice:**

- [redacted]
-
- [redacted]

- **Examples:**

-
-
-
-
-

Topic No 10: What Is An Information Security Program?

- **Project definition:**

- [redacted]
[redacted]

- **Program definition:**

- [redacted]
[redacted]

- **Security program:**

-

ISO27001:2013 (ISMS) REQUIREMENTS AND CONTROLS

-

-

Topic No 11: Role of People, Process, and Tech In InfoSec

-
-
-
- **People:**
 -
 -
 -
- **Processes**
 -
 -
 -
 -
 -
 -
- **Technology plays a central role in the Information Security program:**
 -
 -
 -
 -
 -

Topic No 12: Role Of An Information Security Manager

Topic No 13: What Is Information Security Awareness?

- **Ensure employees are aware of :**

- [REDACTED]
- [REDACTED]
- [REDACTED]

- **NIST Special Publication 800-50 (Building An IT Security Awareness & Training Program)**

-
-
-

- **Awareness:**

-
-
-

- **Training:**

- [REDACTED]
-
-

- **Education:**

-
-

- **Don'ts:**

-
-
-

- **Do's:**

-
-

IMPLEMENTATION STEPS

Topic No 14: Leading Security Standards & Frameworks

-
- The diagram illustrates the relationship between PCI DSS and the Payment Card Industry Data Security Standard (PCI DSS). It features a central box labeled "The Payment Card Industry Data Security Standard (PCI DSS)". To the left of this box, there are three bullet points, each followed by a horizontal line. To the right of the box, there are two yellow rectangular boxes, one above the other, with a horizontal line connecting them to the central box.

- **PCI Data Security Standard (DSS):** accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

—

—

- **COBIT:**

—

—

COBIT is the acronym for Control Objectives for Information and Related Technologies. The COBIT framework was created by ISACA to bridge the crucial gap between technical issues, business risks and control requirements.

-

-

•

•

Topic No 15: What Is Information Security Risk?

- [REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]
- **Risk is managed so that:**
 - [REDACTED]
 - [REDACTED]

- **Risk Assessment:**

- [REDACTED]
- [REDACTED]
- [REDACTED]

- **Challenges with risk focused approach:**

-

-

Topic No 16: Information Security Lifecycle

-

-

- **Step 1: Requirements**

-

-

-

- **Step 2: Assess Current Security Posture**

-

-

- **Step 3: Remediation Plan**

-

-

-
-
-
-
-

- **Step 4: Implement Controls**

-
-
-
-
-
-

- **Step 5: Test/Validate**

-
-



- **Step 6: Security Accreditation**

-
-
-
-



- **Step 7: Monitor & Audit**

-
-
-

Topic No 17: Management Commitment

- What is **management commitment**?

—

- ISO2700:2013 (ISMS) Clause 5.1:

- **“Tone at the top”**

—

—

- In practice:

—

—

—

—

Topic No 18: Information Security Responsibility

- Default organizational perception:

—

—

—

- **Security is everyone's responsibility:**

—

—

[Redacted]

—

[Redacted]

—

[Redacted]

- **Security involvement & accountability:**

—

[Redacted]

[Redacted]

—

-

Topic No 19: Cyber Security Breaches

-

—

-

—

-

—

[Redacted]

— 

|

- **Leading Global Reports:**

- [Redacted]
- [Redacted]

Topic No 20: Challenges Of InfoSec Implementation

- **Challenges Of IT:**

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- **Challenges Of InfoSec:**

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- **Pakistan Industry Security Characteristics:**

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Topic No 21: Role Of A Regulator

-
-
- **cybersecurity regulation**
-
- **Role Of Regulator In Cyber Security:**
 -
 -
 -
 -
-
- **Singapore**
 -
 -
 -
- **Pakistan; Ministry of IT (MOIT):**
 -
 -
- **Pakistan; State Bank Of Pakistan (SBP):**
 -
- **Pakistan lacks:**
 -

-
-
-
-

Topic No 22: Status Of InfoSec in Pakistan

-
-
-
-

Global Cyber Security Index 2017 (ITU):

- **Pakistan cyber security posture (industry):**
 -
 -
 -
 -
 -
- **Reasons for poor security posture:**
 -
 -

—

—

- **Changing dynamics (PK):**

—

—

—

- **Pakistan needs:**

—

—

Topic No 23: Solution For InfoSec Improvement (PK)

•

•

- **Solution for strong security posture:**

—

—

—

—

- **Don't repeat the same mistakes:**

—

—

—

—

Chapter 2:

Typical Enterprise IT Architecture & Security Overlay

Topic No 24: Typical Enterprise IT Network

-

-

-

-

—

—

—

—

-

-
-
-
-
-

—

—

—

-
-
-
-

Topic No 25: Major Components: Enterprise IT Network

- **Edge router**
 -
 -
 -
- **NGN FW**

- **DMZ:**
 -
- **IPS:**
 -
 -
- **Distribution switch**
 -
- **Data center switch & FW**
 -
- **Access switch**
 -
 -
- **NAC**
 -
- **SIEM**
 -
- **Vulnerability Manager**
 -
- **System AV**
 -
- **Server HIPS**
- **UTM**
 -
- **Mobile device – MDM**
 -

Topic No 26: OSI Security Architecture

-
-
-
-
-
-
-

-
-
-
-
-
-

- **Security mechanism:**

-
-

-

Topic No 27: New IT Frontiers: Cloud, Mobile, Social, IOT

-

-

Topic No 28: Virtualization Environment Security

-
- **Virtualization security classified into three areas:**

-
-
-

- **Risk # 1 (VM Sprawl)**

-
-

- **Controls:**

-

-

- **Controls:**

- **Risk # 2 (Sensitive Data Within a VM)**

- **Impact:**

- **Controls:**

-

-

-

Topic No 29: Case Study – Enterprise Network (Small Org)

- **Organizational characteristics:**

-

-

-

-

-

-

- **Organizational culture:**

-

-

-

-

- **IT setup:**

-
-
-
-
-
-

- **Security posture:**

-
-
-
-
-
-

- **Security requirement:**

-
-

- **Driving change ?**

-
-
-

- **Security transformation project:**

-
-
-
-
-

- **Conclusion:**

-
-
-

Topic No 30: Case Study – Enterprise (Medium Org)

- **Organizational characteristics:**

-
-
-
-
-
-

- **Organizational culture:**

-
-
-
-
-

- **IT setup:**

-
-
-
-
-
-
-
-

—

- **Security posture:**

—

—

—

—

—

—

- **Security requirement:**

—

—

- **Driving change ?**

—

—

—

- **Security transformation project:**

—

—

—

—

—

- **Conclusion:**

—

—

—

Topic No 31: Case Study – Enterprise (Large Org)

- **Organizational characteristics:**

-
-
-
-
-
-

- **Organizational culture:**

-
-
-
-
-

- **IT setup:**

-
-
-
-
-
-
-

- **Security posture:**

-
-

-
-
-
-

- **Security requirement:**

-

- **Driving change ?**

-
-
-

- **Security transformation project:**

-
-
-
-
-

- **Conclusion:**

-
-

Topic No 32: Structure Of An IT Team

-
-
-
-
-

•

GENERAL STRUCTURE

JOB FUNCTIONS

ADDITIONAL TASKS

LARGE ORG

(150 IT Staff)

-

-

Topic No 33: Objectives, Performance KPIs, Priorities Of IT

-

-

-

-

-

-

- **Performance KPIs:**

-

-

-

- **Priorities of IT:**

-

-

- **General IT teams performance in Banking:**

-

-

-

- **General IT teams performance in Telcos:**

-

-

-

- **General IT teams performance in Enterprise:**

-

-

- **Security posture:**

-

-

Topic No 34: IT Team Interaction With Other Stakeholders

-
-
-
-
-
-
- -
 -
- **Business requirements & new projects:**
 -
 -
 -
 -
- **Audit & compliance requirements:**
 -
 -
 -
 -
- **Expansion (branches) & maintenance:**
 -
 -
- **IT support for computing (helpdesk):**
 -
 -
 -
- **Business continuity & DR:**
 -
 -

Topic No 35: Security Overlay Of Enterprise (Part 1)

-

Topic No 36: Security Overlay Of Enterprise (Part 2)

-

-

Topic No 37: Security Overlay Of Enterprise (Part 3)

-

More Advanced Security:

-
-
-
-
-
-

Even More Advanced Security:

-
-
-
-
-

Further guidelines for strong security controls:

-

-

—

Topic No 38: High Availability (HA)

- **What is high availability (HA) ?**

—

•

•

•

—

—

—

—

•

—

•

—

Topic No 39: High Availability Design

-

-

Topic No 40: Site Redundancy

-
-
-
- **Hot site (expensive):**
 -
 -
 -
 -
- **Cold site (cheapest):**
 -
 -
 -
- **Warm site (middle ground):**
 -
 -
 -

- **RTO:**

—

- **RPO:**

—

- **Example:**

—

—

Topic no 41: High Availability & Redundancy Case Study

-

-

-

-

-

IT setup:

—

—

—

—

—

—

Primary DC:

—

—

—

Secondary DC (ISB):

-
-
-
-

DR site

-
-
-
-
-
-
-

Backup strategy:

-
-
-
-

Topic no 42: Backup Strategies

• Backup considerations:

-
-
-
-
-
-
-

- **What to backup?**

-
-
-
-

- **Backup location?**

-
-
-

- **Backup frequency?**

-

- **Backup operator and checker?**

-
-
-

- **Backup testing & security considerations:**

-
-

- **Backup tools and technology:**

-
-
-
-
-

Topic no 43: Security Tools Used In An Enterprise

- **Typical security tools used in an enterprise:**

-
-
-
-
-

- **Typical security tools used in an enterprise:**

-
-
-
-
-
-
-

Topic no 44: Security Tools – Typical Enterprise (Part 1)

-
-

- -
 -
 -
 -

Topic no 45: Security Tools – Typical Enterprise (Part 2)

-
-

- **Gartner**
- **Forrester**
- **NSS labs**
- **ICSA Labs**

Topic no 46: What Does “Box Security” Mean?

-
- **Box for :**

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-

Other challenges with “box security” approach:

-
-

-
-
-

Topic no 47: Best Approach: IT Enterprise Security

-
-

Security hardening:

Vulnerability management:

-
-

Security engineering:

Security governance

Topic no 48: What Is Disaster Recovery (DR)?

- **What is a disaster?**

—

- **What is disaster recovery (DR)?**

—

- **What could cause the invocation of a DR fail over to DR site?**

—

—

- **What is the difference between DR and business continuity (BC)?**

—

- **Three step process:**

—

—

—

- **What is a DR plan?**

—

- **DR plan checklist:**

-
-
-
-
-
-
-
-
-

Topic no 49: What is Business Continuity (BC)?

- **What is business continuity?**

-

(Source: ISO 22301:2012)

- **What is business continuity management?**

-

(Source: ISO 22301:2012)

- **What is a BC plan?**

—

—

—

Topic no 50: DR In Enterprise Architecture – Part 1

- **DR considerations:**

—

—

- **DR plan:**

—

—

—

—

—

—

—

—

—

—

- **RTO:**

-

-

- **RPO:**

-

-

Topic no 51: DR In Enterprise Architecture – Part 2

-

-

-

-

-

- **DR facility:**

-

-

-

-
-
-

- **DR drills & testing:**

-
-
-

- **DR testing checklist:**

-
-
-
-
-
-
-
-
-
-
-

- **BC plan alignment:**

-
-
-

Topic no 52: Role Of An IT Asset In Enterprise Security

- **What is an IT asset?**

—

•

-
- **Acceptable Use (Of IT Assets):**

-
-
-
-
-
-

Topic no 53: How To Determine Security Posture?

-
-
-
-
-
-
-
-
-
-
-
-
-
-

Topic no 54: Driving Successful Security Transformation

- -
 -
 -
-

-

Chapter 3

Security Transformation Stage

Topic no 55: Revisit Of Security Transformation Model

- **Security hardening:**

-

-

-

- **Patching:**

-

-

- **Patching considerations:**

-

-

-

- **Hardening:**

- **Note that both hardening & patching are required**

-

-

Topic no 56: Security Hardening Strategy

-

-

-

-

-

-

-

-

-

Topic no 57: Pre-requisites For Security Hardening

1. Security program approved

-
-
-
-
-

2. Consultant on board

-
-

-

-

3. Project kick-off meeting held

-

-

-

-

4. ISMC team identified and their loading for this project communicated

-

-

-

-

5. Appraisal linkage of core resources announced by CIO

-

-

-

Topic no 58: Who Will Conduct The Security Hardening?

- **Involvement of various stakeholders for security hardening**

-

-

-

-

-

- **IT Operations teams:**

-
-
-
-

- **InfoSec team:**

-
-
-
-

- **IT management:**

-
-
-

- **Consultant or project director:**

-
-
-

- **Business stakeholders:**

-

-

Topic no 59: 8 Step Methodology – Security Hardening (1)

-

- **Purpose:**

-

-

- **Benefits:**

-

-

-

-

- **If You Skip This Process:**

-

-

—
—
—

Topic no 60: 8 Step Methodology – Security Hardening (2)

- **Step 1: Identify Critical Assets & Asset Owner:**

-
-
-
-
-

- **Step 2: Research on applicable security controls**

-
-
-
-
-

- **Step 3: Checklist of applicable security controls**

-
-
-

- **Step 4: Document controls into SOP**

-
-
-

Topic no 61: 8 Step Methodology – Security Hardening (3)

- **Step 5: Implement controls on test setup**

-
-
-

—

- **Step 6: Validation of control implementation (by InfoSec team)**

—

—

—

- **Step 7: Change management process for PRODUCTION:**

—

—

—

- **Step 8: Implement on PROD & monitor:**

—

—

—

Topic no 62-65: A Look At CIS Security Benchmarks (1)

-

—

—

•

•

-
-

- **Control content:**

-
-
-
-
-
-
-

- **1.8 (page 88); Session Timeout**

-
-
-

- -

-
-
- -
 -
 -
 -

- **Level 1:**

- -
 -

- **Level 2:**

- -
 -

- **Control content:**

- -
 -
 -

-
-
-
-

- **1.1.2 [L1]:** *Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)*

- *Profile applicability: Level 1 Domain Controller, Level 1 Member Server*

- **1.1.2 [L1] Description:**

-
-

- **1.1.2 [L1] Audit:**

-

•

•

-

Topic no 66: A Look At DISA STIGs (1)

•

•

•

•

•

-
-
-
-
-
-

STIGs HOME

STIGs Master List

STIGs Viewer

STIG Viewer Download

STIG Library Compilation

STIG Viewer Window

Import STIG

-

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

- **STIG content:**

-

-

-

-

-

- **Checklist screens:**

—

—

—

—

—

- **Checklist screens (STATUS):**

—

—

—

—

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

- -
 -

- **Rule Title:**

—

—

- **Discussion:**

—

- **Check Content:**

—

—

—

- **Fix Text:**

—

—

—

Topic no 69: A Look At DISA STIGs (4)

-
-
-

- **General Information:**

- **Rule Title:**

- **STIG ID**

- **Severity**

- **Discussion:**

-

- **Check Content:**

-

—

- **Fix Text:**

—

Topic no 70: Comparison of CIS Vs DISA

-
-
-

- **How to select CIS/DISA:**

-
-
-
-
-

- **Rule of thumb:**

-
-
-
-

Topic no 71: Security Hardening – Windows Server 2012R2

-
-
-
-

- - **Rule Title:**
 - **STIG ID**
 - **Severity**
- **Discussion:**
 -
 -
 -
- **Check Content:**
 -
 -
 -
 -
 -
- **Fix Text:**
 -
- **CCI (Control Correlation Identifier):**
 -

Topic no 72: Case Study Security Hardening – Linux

-

-

-

- *Ensure SSH Protocol is set to 2 (Scored)*

-

-

-

- *Ensure SSH Protocol is set to 2 (Scored)*

-

-

-

- # grep "^Protocol" /etc/ssh/sshd_config Protocol 2**

-

- Protocol 2**

- **Critical Controls:**

-

–

Topic no 73: Security Hardening – Case Study – Solaris

•

•

–

- **General Information:**

- **Rule Title:**

- **STIG ID**

- **Severity**

- **Discussion:**

-

- **Check Content:**

-

- # cat /etc/shells | xargs -n1 ls -lL

-

- # find / -name "*sh" | xargs -n1 ls -lL

-

-

- **Fix Text:**
 -
 - **#chmod 0755 <shell>**
- **CCI (Control Correlation Identifier):**

–

–

–

–

Topic no 74: Case Study Security Hardening – Apache

-
-
-
- **7.7 (page 65); *Configure log file size limit (Scored)***
- **Profile applicability:**
 -
 - **Description:**
 -
 - **Audit:**

- **Remediation:**

java.util.logging.FileHandler.limit=10000

–

Topic no 75: Security Hardening – Case Study – Oracle

-
-

–

- **General Information:**

- **Rule Title:**
- **STIG ID**
- **Severity**

- **Discussion:**

–

–

–

- **Check Content:**

-

-

-

-

Oracle[ORACLE_HOME_NAME]TNSListener

- **Fix Text:**

-

- **For example**

-

- **CCI (Control Correlation Identifier):**

-

-

-

-

Topic no 76: Case Study Security Hardening – MS SQL

-

-

-

- *2.14 Ensure 'sa' Login Account has been renamed (Scored)*

- **Profile applicability:**

-

- **Description:**

- **Rationale:**

- **Audit:**

SELECT name FROM sys.server_principals WHERE sid = 0x01;

- **Remediation:**

ALTER LOGIN sa WITH NAME = <different_user>;

- **Impact:**

- **Default Value:**

Topic no 77: Security Hardening – Case Study – Oracle

-

-

-

- **General Information:**

- **Rule Title:**
- **STIG ID**
- **Severity**

- **Discussion:**

-
-

- **Check Content:**

- **name = 'remote_os_roles';**
-

- **Fix Text:**

-
-
- **alter system set remote_os_roles = FALSE scope = spfile;**
-

- **CCI (Control Correlation Identifier):**

-
-
-
-

Topic no 78: Case Study Security Hardening – Windows 8

-
-
-
- *18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)*
- -
 -
- *18.9.70.3 Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (Scored)*
- -
 -
 -
- **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsErrorReporting:AutoApproveOSDumps**

Topic no 79: Case Study Security Hardening – Win 10

-
-

–

- **General Information:**

- **Rule Title:**
- **STIG ID**
- **Severity**

- **Discussion:**

- **Check Content:**

–

–

- **Fix Text:**

–

–

Topic no 80: Case Study Security Hardening – MS Exchange

-
-
-
- 2.5 Set 'Do not permanently delete items until the database has been backed up' to 'True' (Scored)
- - Level 1
 - Description:
 - Rationale:
 - Audit:

RetainDeletedItemsUntilBackup

Get-MailboxDatabase <Mailbox Database Name> | fl -property RetainDeletedItemsUntilBackup
 - Remediation:

Set-MailboxDatabase <Mailbox Database Name> -RetainDeletedItemsUntilBackup \$true
 - Impact:
 - Default Value:

Topic No 81: Security Hardening – Case Study – AD

-
-

–

- **General Information:**

- **Rule Title :**

- **STIG ID**

- **Severity**

- **Discussion:**

-

–

- **Check Content:**

-

-

- **Fix Text:**

–

- **CCI (Control Correlation Identifier):**

Topic No 82: Case Study Security Hardening – IE Browser

-

-

-

- *1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)*

-

–

- **Description:**

-

-

-

- **Rationale:**

- **Audit:**

- **Remediation:**

Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Do not allow users to enable or disable add-ons

- **Impact:**

- *1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)*

-

Topic No 83: Security Hardening – Case Study - Chrome

-

-

-

- **General Information:**

- **Rule Title :**

-

- **Vuln ID:**

- **STIG ID**

- **Severity**

- **Discussion:**

-

- **Check Content:**

- **Universal method:**

- **Windows method:**

- **Fix Text:**

- **CCI (Control Correlation Identifier):**

-

Topic No 84: Case Study Security Hardening – Firefox

-

-

-

- 3.5 (L2) Enable IDN Show Punycode (Scored)

-

-

- **Description:**

- **Rationale:**

- **Audit:**

- `network.IDN_show_punycode=true`

- **Remediation:**

- `lockPref("network.IDN_show_punycode", true);`

- **Default Value:**

Topic No 85: Security Hardening – Case Study – FW

-
-

- - Rule Title :
 - Vuln ID:
 - STIG ID
 - Severity

- Discussion:

–

–

- Check Content:

–

–

- Fix Text:

–

- CCI (Control Correlation Identifier):

–

Topic No 86: Security Hardening – Case Study – Switch

-
-

—

- **General Information:**
 Rule Title :

- **General Information:**
 - **Vuln ID:**
 - **STIG ID**
 - **Severity**

- **Discussion:**

—

- **Check Content:**

—

switchport port-security violation shutdown

- **Fix Text:**

—

Topic No 87: Case Study Security Hardening – Cisco IOS 15

-
-

-
-
- 3.3.2.2 Set 'ip ospf message-digest-key md5' (Scored)
-

—

— **Description:**

— **Rationale:**

— **Audit:**

hostname#sh

run int {*interface*}

— **Remediation:** C

hostname(config)#interface {*interface_name*} hostname(config-if)#ip ospf message-digest-key {*ospf_md5_key-id*} md5 {*ospf_md5_key*}

— **Impact:**

— **Default Value:**

Topic No 88: Security Hardening – Case Study – WLAN

-
-
-

- - **Rule Title :**
 - **Vuln ID:**
 - **STIG ID**
 - **Severity**

- **Discussion:**

–

–

–

- **Check Content:**

-

-

-

- **Fix Text:**

-

-

Topic No 89: Security Hardening – Case Study – L3 Switch

-

-

-

- **General Information:**

- **Rule Title :**

- **Vuln ID:**

- **STIG ID**

- **Severity**

- **Discussion:**

-

-

—

- **Check Content:**

—

- **Fix Text:**

—

Topic No 90: Case Study Security Hardening – VMware

-

-

-

- *5.1 Disable DCUI to prevent local administrative control (Scored)*

-

—

- **Description:**

- **Rationale:**

—

– **Audit:**

List DCUI settings for all hosts Get-VMHost | Get-VMHostService | Where { \$_.key -eq "DCUI" }

• **Remediation:**

• **Impact:**

–

• **Default Value:**

–

Topic no 91 & 92 : Software Security Fundamentals-SAMM & SAMM-2

- -
 -

- -
 -
 -

Governance Phase:

- **Strategy & Metrics:**

-

-

- **Education & Guidance:**

-

-

- **Policy & Compliance:**

-

-

Topic no 93

-

Construction Phase:

-

-

—

- **Security Requirements:**

—

—

- **Threat Assessment:**

—

—

- **Secure Architecture:**

—

—

Topic no 94: SECURITY HARDENING – SOFTWARE APPLICATIONS

- **Two types of security hardening:**

-

-

- **Typical enterprise software:**

-

- **Internally or 3rd party developed software in ASP.NET, PHP, Android/IOS, or other platform**

- **Useful resources:**

-
-
-
-
-
-

- **Conclusion**

-

-

-

-

Topic no 95: CASE STUDY – ASP.NET SECURITY HARDENING

-
-
-
-
-
- **.NET Framework Guidance**
 -
 -
 -
- **NET FRAMEWORK, DATA ACCESS GUIDANCE:**
 -
 -
 -
 -
 -
 -
 -
- **.NET FRAMEWORK, GENERAL GUIDANCE:**
 -
 -
 -
 -
- **ASP.NET Web Forms Guidance**

-
-
-

- **ASP.NET MVC Guidance**

-
-

Topic no 96: CASE STUDY – PHP SECURITY HARDENING

-
-

-
-
-
-

-
-
-
-
-

9. PHP Configuration

- **Error Reporting**

Topic no 97: CASE STUDY – ASP.NET MVC SECURITY HARDENING

-
-
-
-
-
-

A.6 Sensitive data exposure

-
-
-

–

–

–

–

–

–

–

Topic no 98: Security Hardening – Case Study-SharePoint

•

•

–

•

•

– **Rule Title :**

– **Vuln ID:**

- **STIG ID**

- **Severity**

- **Discussion:**

-

-

- **Check Content:**

-

-

-

-

- **Fix Text:**

-

Topic no 99: CASE STUDY – C APPLICATIONS SECURITY HARDENING

-
-
-

-
-

•

•

—

—

—

—

Topic no 100: CASE STUDY – C++ APPLICATIONS SECURITY HARDENING

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

-

- **Non-Compliant Code Example:**

-

-

- **Compliant Code Example:**

-

Topic no 101: CASE STUDY – JAVA APPLICATIONS SECURITY HARDENING

-

-

- **Rule 7**

-

-

- **Non-compliant Code Example:**

-

-

- **Compliant Solution:**

–

–

Topic no 102: CASE STUDY – PERL APPLICATIONS SECURITY HARDENING

-

-

- **Rule 1**

-

-

-

- **noncompliant code example**

- **compliant code example**

Topic no 103: Case Study Security Hardening – Android

-
-
-
- *1.15 Ensure Android Device Manager is set to Enabled (Not Scored)*
- -
 - **Description:** **Android Device Manager**
- **Rationale:**
 -
- **Audit:**
- **Remediation:**

- **Impact:**

-

- **Default Value:**

-

Topic no 104: Case Study Security Hardening – Apple IOS 10

-

-

-

- *3.2.1.12 (L2) Ensure 'Allow modifying cellular data app settings' is set to 'Disabled' (Not Scored)*

- **Profile applicability:**

-

- **Description:**

- **Rationale:**

-

- **Audit:**

-

-
-
-
-
-
-

- **Remediation:**

-
-
-
-

modifying cellular data app settings.

-

Allow

- **CIS Controls:**

-
-

Topic no 105: CASE STUDY – ASTERISK VOIP SECURITY HARDENING

1. Physically secure your IP PBX and network hardware

-

2. Never, Never, Never use the default passwords on any system. (Use Strong Passwords)

-

3. Never use the same Username and password on your extensions

-

4. Place your PBX behind a Firewall

-
-
-

5. Use the “permit=” and “deny=” lines in sip.conf

-

6. Keep inbound and outbound routing separate (asterisk)

-

Topic no 106: CASE STUDY – ASTERISK VOIP SECURITY HARDENING (2)

7. Limit registration by extensions to your local subnet.

-

8. Disable channels and services that are not in use

-

9. Make it harder for sip scanners (Set “alwaysauthreject=yes”)

-

-

10. Limit and restrict routing and phone number dial plans

-

11. Audit your system security regularly

Topic no 107: Version Control For IT Assets

-
-
- **Benefits of version control**
 -

- -
 -
 -

Topic no 108: Version Control Best Practices

- **Version control best practices**

—

Topic no 109: SECURITY HARDENING - SECURE SOFTWARE IMAGES

-
-
-

5.1 Establish Secure Configurations

-

5.2 Maintain Secure Images

-

5.3 Securely Store Master Images

-

5.4 Deploy System Configuration Management Tools

-

5.5 Implement Automated Configuration Monitoring Systems

-

Topic no 110: SECURITY HARDENING – MANUAL & AUTOMATED WORK

-
- **Step 1:**
 -
- **Step 2:**
- **Step 3:**

-
- Step 4:
- Step 5:

-
-
-

Topic no 111 & 112 : QUALYS DEMO – SECURITY HARDENING

-

-

-

Topic no 113: SECURITY HARDENING – LIFECYCLE

-

1: Harden IT Asset

2: Periodic Validation

3: Seek Updated On Hardening Benchmarks

-

-

4: Implement Additional Controls

-

5: Pursue & Implement Controls That May Require Additional Working

-

-

-

Topic no 114: Hardening When CIS/DISA STIG Not Available

- -
 -

- **Step 2: Research:**

- -

- **Other considerations:**

- -
 -
 -
 -

-

Topic no 115: QUALYS POLICY LIBRARIES

-
-
-
-
-
-

-

Topic no 116: Security Hardening For Outsourced IT Assets

-
-
-
- **IT Outsourcing examples:**
 -
 -
 -
 -
 -
 -
- **Mechanism:**
 -
 -
 -
 -
 -
- **Important considerations:**
 -
 -
 -
 -
- **Security evaluations:**
 -
 -
 -
 -

Topic no 117: What is Vulnerability Management?

- **What is vulnerability?**
 -

- **How do you fix vulnerabilities?**
 -

- **What is vulnerability management?**
 -

- **What is vulnerability assessment (VA)?**
 -

- **What are some of the common vulnerability scanners?**
 -
 -
 -
 -

Topic no 118: What Are The Steps In VM Lifecycle?

VM Steps:

1. Analyze Assets:

-
-
-
-

2. Prepare Scanner:

-
-
-
-
-
-

3. Run Vulnerability Scanner:

-
-
-

4. Assess Results:

-
-
-
-

5. Patch Systems:

-
-
-
-
-

6. Verify (Re-scan)

-
-
-

Topic no 119: Why Is Software Insecure?

-
-
-
- **Result:**
- - **Connectivity;**
- **Extensibility:** “
-
- **Complexity:**
-
- **Monoculture: Dan Greer:**

Topic no 120: Why Is A VM Program Required?

- **What is a patch?**
 - **patch**
security
- **What is patch management?**
 -
- **Patch management tasks :**
 -
- **Risk of not patching:**
 -

-

-

Topic no 121: What Is CVE & Vulnerability Database?

- **What is CVE?**

-

- **What is NVD?**

-

- **What is the NVD severity score?**

-

-

- -
 -
 -
 -

Topic no 122: What Is An Exploit?

- **What is an exploit?**

-

- **Remote exploit:**

- *remote exploit*

- **Local exploit:**

- *local exploit*

- **Exploit database:**

-

-

exploits and proof-of-concepts rather than advisories

- **Zero-day exploit:**

—

exploit

Topic no 123: Effective Vulnerability Management: Stage 2

-

—

—

—

—

—

-

-

-

-

-

-

Topic no 124: Security Breach Case Study 1: Home Dept 2014

-

-

-

-

-

-

-

-

-

-

-

-

Topic no 125: Security Breach Case Study 2: Anthem

-

-

- **Sequence of events:**

-

-

-

-

-

- **Vulnerabilities:**

-

-

- **Remediation measures:**

-

-

Topic no 126: Best Practices For Applying Security Patches

-

-

- 1. Use a change control process**

-

-

2. Read all related documentation:

–

–

–

–

–

Topic no 127: Who Conducts Vulnerability Management

•

- **Role of Infosec team:**

-
-
-
-
-
-
-

- **Role of IT Ops team:**

-
-
-
-
-
-
-
-
-
-
-

Topic no 128: Nessus Features

-
- -
 -
 -
- -
 -
 -
- -
 -
- -
-
-
-

Topic no 129: Qualys Features

•

|
|
|
|
|
|
|
|
|
|

- -
 -
 -

-
-
-

Topic no 130: Nessus Demo – 1

-
-
-
-

LOGIN SCREEN

DASHBOARD

NEW SCAN

WANNACRY RANSOMWARE SCAN

NEW SCAN WINDOW

DASHBOARD VIEW WITH SCANS

NEW SCAN...

ENTER SCAN DETAILS

CREDENTIAL SCAN

COMPLIANCE SCAN

WINDOWS COMPLIANCE MENU (CIS)

WINDOWS COMPLIANCE MENU (CIS)...

-
-
-
-

Topic no 131: Nessus Demo – 2

-
-
-
-

- **ADVANCED SCAN / COMPLIANCE**

ADVANCED SCAN / PLUG-INS

SCAN...IN PROGRESS

SCAN REPORT [43 INFO]

SCAN REPORT [DETAILS]

SCAN REPORT [DETAILS...]

WEB APPLICATION TEST

WEB APPLICATION TEST - CREDENTIALS

CREDENTIALIALED PATCH AUDIT

CREDENTIALIALED PATCH AUDIT

SCANS DASHBOARD

- **CREDENTIALAED AUDIT SCAN RESULTS [61 INFO]**

Topic no 136: How Do VM Scanners Work?

-
-
-
- Checking if the remote host is alive
-
-
- Firewall detection
-
- TCP / UDP Port scanning
-

- **OS Detection**
-
-
- **TCP / UDP Service Discovery**
-
- **Vulnerability assessment based on the services detected**
-
-
- **Limitations:**

Topic no 139: Open Source Vulnerability Scanners

-
-
-

APPROXIMATELY 50k NETWORK VULNERABILITY TESTS

-
-

Topic no 140: Suggested Frequency For VM Scanning

- **Pre-requisites**

-
-
-
-

- **At the start:**

-
-
-
-

- **As organizations get more mature in scanning discipline:**

-
-
-

- **Mature organizations:**

-
-
-
-

- **Most mature organizations:**

-
-
-

Topic no 141: VM Challenges & Pitfalls

- **Challenges:**

-
-
-
-

- **Internal expertise on VM tool**
 -
 -
 -
 -
 -
- **Not enough support from IT teams:**
 -
 -
 -
- **Patching causing application failure:**
 -
 -
 -
- **Not enough management support:**
 -
 -
 -

Topic no 142: IT Asset Management Challenges

-
-
- **Challenges:**
 -
 -
 -
 -
 -

- **Asset discovery & tracking**

-
-
-
-
-

- **Antivirus status:**

-
-
-

- **Windows & OS updates:**

-
-
-
-
-

- **Patch management:**

-
-
-
-
-

- **Change management:**

-
-
-

Topic No 144: ASSET MANAGEMENT TOOLS FOR SECURITY FUNCTIONS

-

-

-

-

-

-

-

Topic No 145: WHAT IS SECURITY ENGINEERING?

-

-

-

- **Types of activities for security engineering:**

-

-

-

-

-

- **DMZ Architecture Case Study:**

-

-

-

- **FW Access List Case Study:**

-
-
-

- **Why at Layer 3 of Security Transformation Model?**

-
-
-

Topic No 146: WHAT IS THE OBJECTIVE OF SECURITY ENGINEERING?

-
-
-
-
-

-
-
-

-
-

-

-

Topic No 147: WHOSE RESPONSIBILITY IS SECURITY ENGINEERING?

-

-

Topic No 148: CIS 20 CRITICAL SECURITY CONTROLS

-

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Topic No 149: CSC1: Inventory Of Authorized & Unauthorized Devices

1.1:

1.2:

1.3:

1.4:

–

–

–

1.5:

1.6:

Topic No 150: CSC2: Inventory Of Authorized & Unauthorized Software

2.1:

2.2:

–

–

2.3:

–

–

2.4:

Topic No 151: CSC3-I: Secure Configurations For HW & SW

3.1

–

–

3.2:

–

–

–

3.3:

–

3.4:

–

Topic No 152: CSC3-II: Secure Configurations For HW & SW

3.5:

–

–

3.6:

–

–

3.7:

Active Directory Group Policy Objects
Puppet for UNIX systems

–

Topic No 153 & 154: CSC4-I: Continuous Vuln. Assessment & Remediation

4.1:

–

–

4.2:

–

–

4.3:

–

–

4.4:

–

4.5:

–

4.6:

4.7:

–

4.8:

–

–

–

Topic No 155: CSC5-I: Controlled Use Of Administrative Privileges

5.1

5.2

5.3

5.4

5.5

5.6:

5.7:

5.8

5.9:

Topic No 163: CIS CONTROL 9: LIMITATION & CONTROL OF NETWORK

CIS 20 Critical Security Controls

9.1: Associate Active Ports, Services and Protocols to Asset Inventory

-

9.2: Ensure Only Approved Ports, Protocols and Services Are Running

-

9.3: Perform Regular Automated Port Scans

-

9.4: Apply Host-based Firewalls or Port Filtering

-

9.5: Implement Application Firewalls

-

PROCEDURES & TOOLS:

-

-

Topic No 163: CIS CONTROL 10: DATA RECOVERY CAPABILITIES

10.1: Ensure Regular Automated Back Ups

-

10.2: Perform Complete System Backups

-

10.3: Test Data on Backup Media

-

10.4: Ensure Protection of Backups

-

10.5: Ensure Backups Have At least One Non-Continuously Addressable Destination

-

Procedures & Tools:

-

-

Topic No 236: ISO31000:2018 – RISK MANAGEMENT – PROCESS

Topic No 237: ISO31000:2018 – RISK MANAGEMENT – HOW TO IMPLEMENT

Plan:

Implement:

Measure:

Learn

Topic No 238 & 239: INCIDENT MANAGEMENT- I & II

-

-

1. Audit & Due Diligence

-

-

-

2. Create Response Team

-

-

-

-

3. Create Documented IR Plan

-

-

4. Identify Indicators & Triggers

-

-

-

5. Investigate the Problem

-

-

-

-

-

6. Triage & Mitigation

-

-

-

7. Recovery

-

8. Documentation & Reporting

-

9. Process Review

-
-

10. Practice, Practice, Practice

-

Topic No 240: CHANGE MANAGEMENT-I

Types Of Changes

Standard changes

-
-

Normal Changes

- T

Emergency Changes

-