Smarter education for smarter planet

IBM Innovation Centre for Education

Introduction to IT system security

Unit objectives

After completing this unit, you should be able to:

- Get an overview of IT system security
- Understand need of IT system security
- Get familiar with technical controls in IT system security
- Gain insight on system security risk management
- Understand transformation trends

What is IT system security?

- IT system security covers everything from prevention, detection and response to improper access from within and outside an organization, to protect information and systems
- As the critical importance of IT systems grows daily, so does the volume of targeted attacks, internal fraud and other security risks from which IT systems need to be defended.
- Elements of IT system security
  - Vulnerability
  - Threat
  - Risk
  - Exposure
  - Countermeasure or Safeguard
  - The Relation Between the Security Elements

Threats to IT systems (1 of 3)

#	Category of Threat	Examples
1	Compromises to intellectual property	Piracy, copyright infringement
2	Software attacks	Viruses, worms, macros, denial of service
3	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4	Espionage or trespass	Unauthorized access and/or data collection

Threats to IT systems (1 of 3)

#	Category of Threat	Examples
5	Forces of nature	Fire, flood, earthquake, lightening
6	Human error or failure	Accidents, employee mistakes
7	Information extortion	Blackmail, information disclosure
8	Missing, inadequate, or incomplete controls organizational policy or planning	Loss of access to systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place

Threats to IT systems (3 of 3)

#	Category of Threat	Examples
9	Missing, inadequate, or incomplete controls	Network compromised because of absence of firewall controls
10	Sabotage or vandalism	Destruction of systems or information
11	Theft	Illegal confiscation of equipment or information
12	Technical hardware failures or errors	Equipment failure
13	Technical software failures or errors	Bugs, code problems, unknown loopholes
14	Technological obsolescence	Antiquated or outdated technologies

Technical controls in IT system security (1 of 3)

- Identification and Authentication
  - Identification and Authentication Based on Something the User Knows
    - Passwords
    - Cryptographic Keys
  - Identification and Authentication Based on Something the User Possesses
    - Memory Tokens
    - Smart Tokens
  - Identification and Authentication Based on Something the User Is

Technical controls in IT system security (2 of 3)

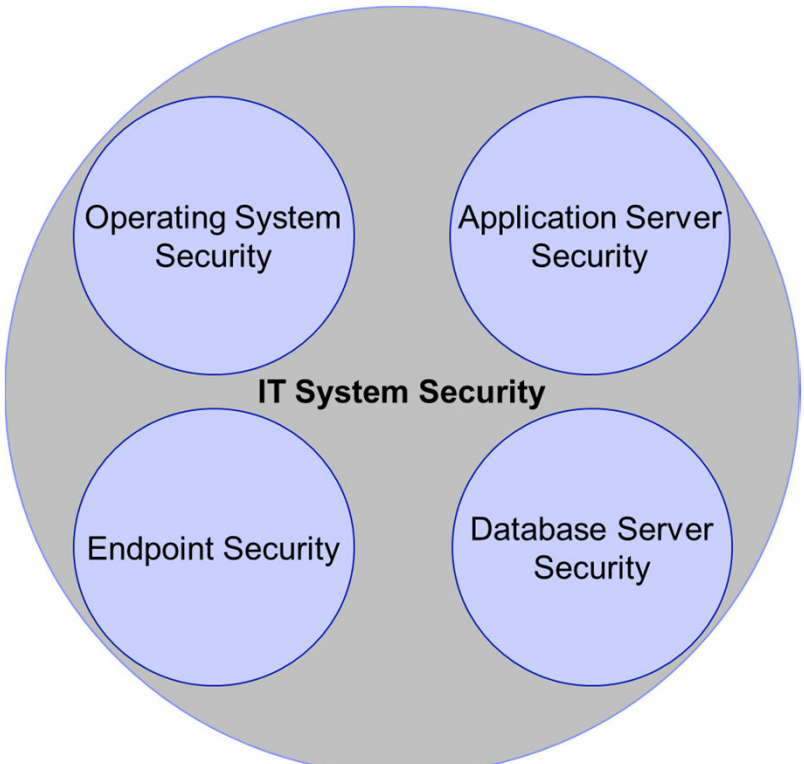
- Logical Access Control
  - Access Criteria
    - Passwords
    - Access Control Lists
    - Encryption
    - Constrained User Interfaces
    - Security Labels
  - Policy: The Impetus for Access Controls
    - Memory Tokens
    - Smart Tokens
  - Technical Implementation Mechanism
    - Internal Access Controls
    - External Access Controls
  - Administration of Access Controls
    - Centralized Administration
    - Decentralized Administration
    - Hybrid Approach
  - Coordinating Access Controls

Technical controls in IT system security (3 of 3)

- Cryptography
  - Basic Cryptographic Technologies
    - Secret Key Cryptography
    - Public Key Cryptography
    - Hybrid Cryptographic Systems
    - Key Escrow
  - Uses of Cryptography
    - Data Encryption
    - Integrity
    - Electronic Signatures
    - User Authentication

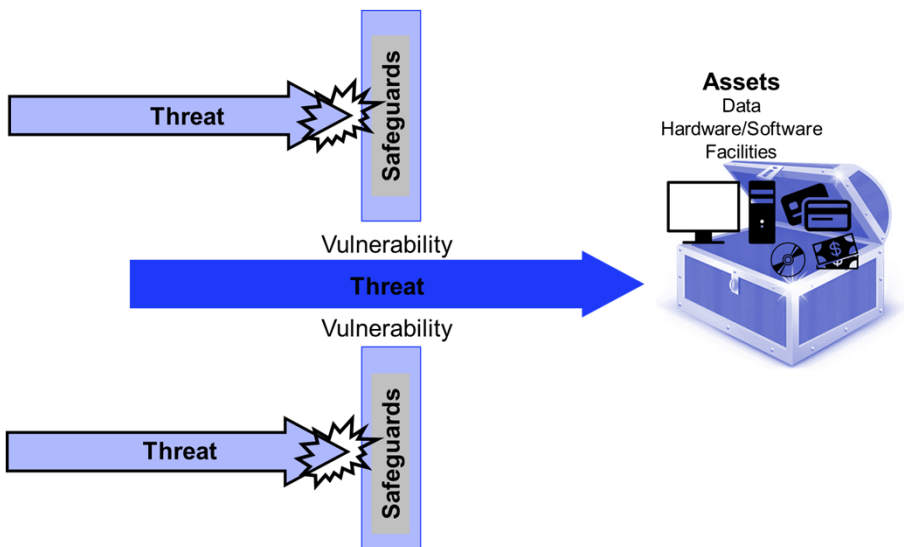
Distinct features	Secret key cryptography	Public key cryptography
Number of keys	Single key	Pair of keys
Types of keys	Key is a secret	One key is private, and one key is public
Protection of keys	Disclosure and modification	Disclosure and modification for private keys and modification for public key
Relative speeds	Faster	Slower

System security coverage



System security risk management (1 of 2)

- The process of risk assessment involves following activities:
  - determining the assessment's scope and methodology
  - collecting and analyzing data
  - interpreting the risk analysis results



The interrelationship of vulnerabilities, threats, and assets

System security risk management (2 of 2)

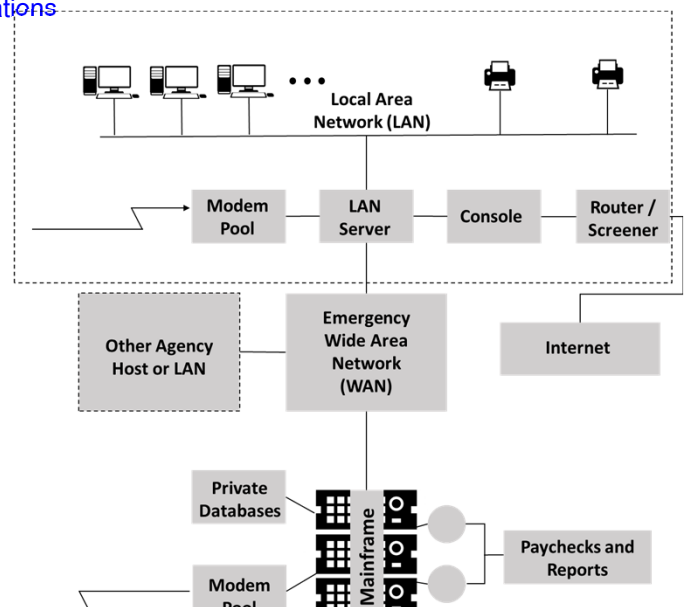
- Risk mitigation: Selection and implementation of security controls
  - Selecting safeguards
  - Accept residual risk
  - Implementing controls and monitoring effectiveness
  - interpreting the risk analysis results

Case study: Context setting

- A hypothetical IT Department in the Ministry of Electronics and Information Technology and how it is dealing with IT security issues in its operating environment.
- Identification of assets
  - System components owned and operated by IT Department
  - Contracting and procurement documents
  - Internal correspondence
  - Draft resolutions
  - Other day-to-day business documents, memos, and reports

Case Study: Analysis of IT Department's System

- Analysis of IT Department's System
  - System Architecture
  - System Operational Authority/Ownership
  - System Applications



System Architecture

Case study: Threat analysis

- Threats posed to different assets of IT Department
  - Payroll fraud
  - Payroll errors
  - Interruption of operations
  - Disclosure or brokerage of information
  - Network-related threats

Examples of Threats to IT Department Systems		
Potential Threat	**Probability**	**Impact**
Accidental Loss/release/disclosure of sensitive information	Medium	Low/Medium
Accidental destruction of information	High	Medium
Loss of information due to virus contamination	Medium	Medium
Misuse of system resources	Low	Low
Theft	High	Medium
Unauthorized access to telecommunication resources	Medium	Medium
Natural disaster	Low	High

Case study: Security measures in place

- Security measures in place at the IT Department
  - Protection against payroll fraud and errors: time and attendance application
  - Protection against unauthorized execution
  - Protection against payroll errors
  - Protection against accidental corruption or loss of payroll data
  - Protection against interruption of operations
    - Network affairs contingency planning
    - Division contingency planning
  - Protection against disclosure or brokerage of information
  - Protection against network-related threats
  - Protection against risks from non–it department systems

Case study: Vulnerability analysis

- Vulnerabilities analysis (reported by the risk assessment team)
  - Vulnerabilities related to payroll fraud
    - Falsified time sheets
    - Unauthorized access
    - Bogus time and attendance applications
    - Unauthorized modification of time and attendance data
  - Vulnerabilities related to payroll errors
  - Vulnerabilities related to continuity of operations
    - Network affairs contingency planning
    - Division contingency planning
    - Virus prevention
    - Accidental corruption and loss of data
  - Vulnerabilities related to information disclosure/brokerage
  - Network-related vulnerabilities

Case study: Vulnerability mitigation

- Vulnerability mitigation
  - Mitigating payroll fraud vulnerabilities
  - Mitigating payroll error vulnerabilities
  - Mitigating vulnerabilities related to the continuity of operations
  - Mitigating threats of information disclosure/brokering
  - Mitigating network-related threats

Checkpoint

1. IT Security goal of “Non-repudiation” guarantees
   A. an operation cannot be refuted
   B. only authorized personnel can have access to systems and no one else
   C. non availability of system to unauthorized people
   D. system’s proper operation
2. In what category would a software fall if it provides a way to an unauthorized individual access to resources within the IT system environment
   A. Threat
   B. Risk
   C. Vulnerability
   D. Based on the resources involved, it can be a threat or a vulnerability
3. What threat does a “phreaker” pose to an organization’s IT system?
   A. Disrupt services involving public telephone network
   B. Injecting a malware in the IT network
   C. Remove software protection
   D. None of the above

Checkpoint

4. Which of the following is not true about a memory token?
   A. Memory tokens process information after storing it
   B. A magnetic striped card is an example of memory token
   C. Production of memory tokens is costly
   D. Both B and C
5. Which of the following is a function(s) of a constrained user interface?
   A. Help user to implement system-specific policy with flexibility
   B. Assign privileges to the owner of a system
   C. Restrict users' access to specific functions
   D. Both A and B
6. Which of the following statements is true for secret key cryptography?
   A. Secret key cryptography uses a single key shared by two (or more) parties
   B. Secret key cryptography relies on keeping the key secret
   C. Secret key cryptography is relatively faster than public key cryptography
   D. All of the above

Checkpoint

7. Choose the correct alternative from the following

Assertion (A): Password-based access control is often inexpensive

Reason (R): It is already included in a large variety of applications

   A. Both A and R are true and R is the correct explanation of A
   B. Both A and R are true but R is NOT the correct explanation of A
   C. A is false but R is true
   D. Both A and R are false

8. Encryption can be used in IT system security as a mechanism for
   A. logical access control for systems
   B. protecting information when it is being transmitted over a network
   C. Both A and B
   D. Only B

9. Which of the following is NOT a means of authenticating a user's identity?
   A. A token e.g., an ATM card or a smart card
   B. Handwriting dynamics
   C. A Personal Identification number
   D. None of the above

Checkpoint

10. Which of the following is a drawback of smart tokens

A. They need reader/writers or human intervention
B. They require strong Administration
C. All of the above
D. Both C and D

Checkpoint Solutions

1. A
2. C
3. A
4. A
5. C
6. D
7. A
8. C
9. D
10. D

Unit summary

Having completed this unit, you should be able to:

- Get an overview of IT system security
- Understand need of IT system security
- Get familiar with technical controls in IT system security
- Gain insight on system security risk management
- Understand transformation trends

Operating System Security

Unit objectives

After completing this unit, you should be able to:

- Get to know the threats that are faced by operating systems and how they are evolving
- Understand key security features of operating systems
- Get an insight on the security guidelines for server and workstation operating systems
- Get familiar with threats in various mobile operating systems

Operating System & Changing Threats

- Introduction of Changing Threats
  - Basics of Operating Systems & changing threats
  - Formal security mechanisms in operating system

Why OS is Hard to Secure?

- Explaining why the Operating system is hard to secure
  - OS not able to find themselves prone attacks
  - Multiple peripherals can be externally connected through interfaces, such as integral devices
  - Unlike USB driver and hardware devices developed by the hardware manufacturers, etc.

Securing Operating Systems

- How to secure operating system and its models:
  - Trust Model
  - Threat Model

Key Security Features (1 of 2)

- Defining the various features of security
  - Access control
  - Network protection

Key Security Features (2 of 2)

- Defining the various features of security
  - Malware protection

Operating system history

- Brief histories abut different operating systems
  - Unix
  - Window

Security in Ordinary Operating Systems UNIX (1 of 2)

- Explaining the few security systems in UNIX
  - UNIX Protection System
  - UNIX Authorization

Security in Ordinary Operating Systems UNIX (2 of 2)

- Explaining the few security systems in UNIX
  - UNIX Security Analysis
  - UNIX Vulnerabilities

Security in Ordinary Operating Systems Windows (1 of 2)

- Explaining the few security systems in Windows
  - Windows Protection System
  - Windows Authorization

Security in Ordinary Operating Systems Windows (2 of 2)

- Explaining the few security systems in Windows
  - Windows Security Analysis
  - Windows Vulnerabilities

Server Operating System Security Guidelines

- Here are the guidelines for server operating security system
  - Installation & Configuration
  - OS Hardening
  - Disabling unwanted services and protocols

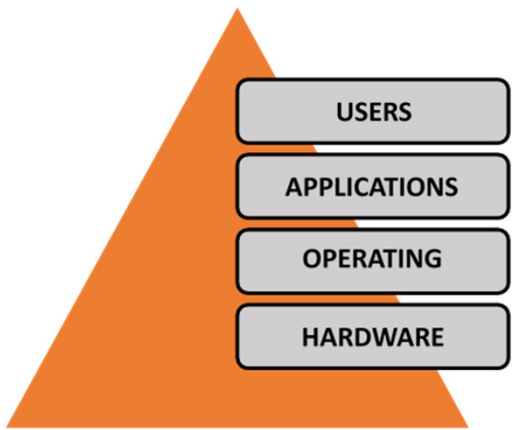
Function	Static ports
Browsing	UDP:137,138
DHCP Lease	UDP:67,68
DHCP Manager	TCP:135
Directory Replication	UDP:138 TCP:139
DNS Administration	TCP:139
DNS Resolution	UDP:53
Event Viewer	TCP:139
File Sharing	TCP:139
Logon Sequence	UDP:137,138 TCP139
NetLogon	UDP:138
Pass Through Validation	UDP:137,138 TCP:139
Performance Monitor	TCP:139
PPTP	TCP:1723 IP Protocol:47
Printing	UDP:137,138 TCP:139
Registry Editor	TCP:139
Server Manager	TCP:139
Trusts	UDP:137,138 TCP:139
User Manager	TCP:139
WinNT Diagnostics	TCP:139
WinNT Secure Channel	UDP:137,138 TCP:139
WINS Replication	TCP:42
WINS Manager	TCP:135
WINS Registration	TCP:137

Workstation Operating System Security Guidelines

- Here are the guidelines for workstation operating security system
  - Installation & Configuration
  - OS and Application S/W Hardening

Mobile Operating Systems

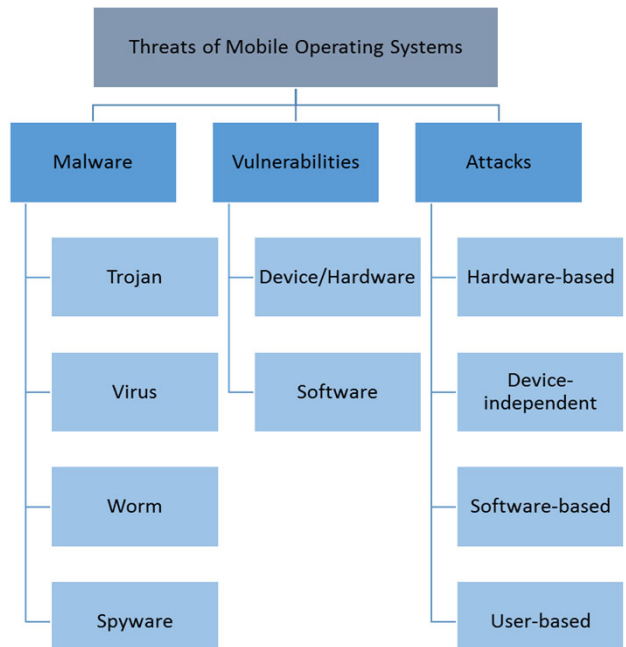
- Explaining the various mobile Operating systems
  - Android Mobile OS
  - Apple Mobile OS
  - Java ME
  - Symbian
  - Windows Phone



Operating System Common Structure

Threats of Mobile Operating Systems

- Some major threats & vulnerabilities of mobile OS
  - Malware
    - Trojans
    - Virus
    - Worm
    - Spyware
  - Vulnerabilities
    - Device-Hardware Vulnerabilities
    - Software Vulnerabilities



Threats of Mobile Operating Systems

- Some major attacks of mobile OS
  - Hardware-based attacks
  - Device-independent attacks
  - Software-based attacks
  - User-based attacks

Lab: Tripwire SecureCheq

- Tool Introduction
  - Tripwire SecureCheq™ tests and remediates Microsoft Windows desktop or server configurations. It particularly
  - Tests for typical and often dangerous Windows configuration errors
  - Provides detailed remediation and repair advice
  - Tests for configuration errors related to OS hardening, data protection, user account activity and audit logging
  - Demonstrates how systems can be continually hardened against attack
- Some features that make it a viable choice for business users include the following:
  - Installs in minutes using a set up and configuration wizard
  - Comprehensive scan results and audit-ready reports in less than an hour
  - Comprehensive policy library that makes it easy to check for compliance
  - On premise deployment gives you complete control
- System Requirements:
  - Hardware
  - Software

Installation (Step -1)

- Download Tripwire_SecureCheq_WS_2003_110 file.

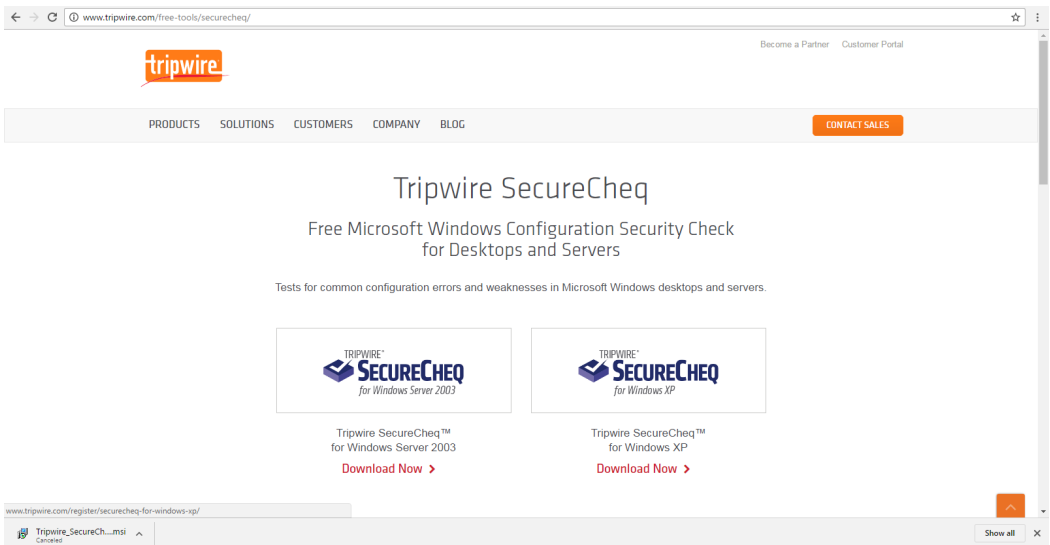
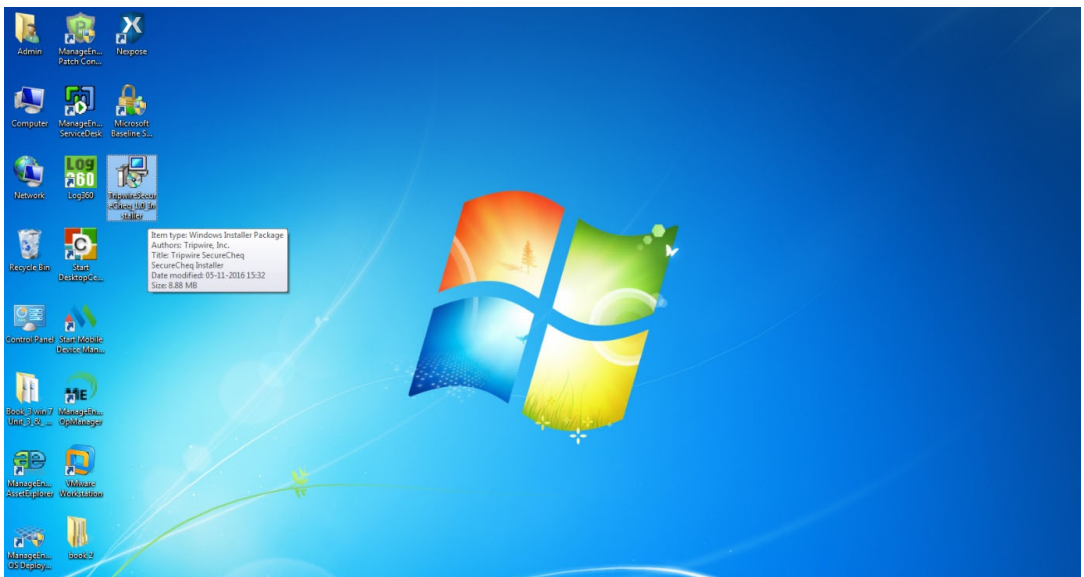


Figure: Download screen

Installation (Step - 2)

- Double click on .msi file of Tripwire SecureCheq to begin the installation. Click on "**Yes**" to run the Tripwire SecureCheq setup

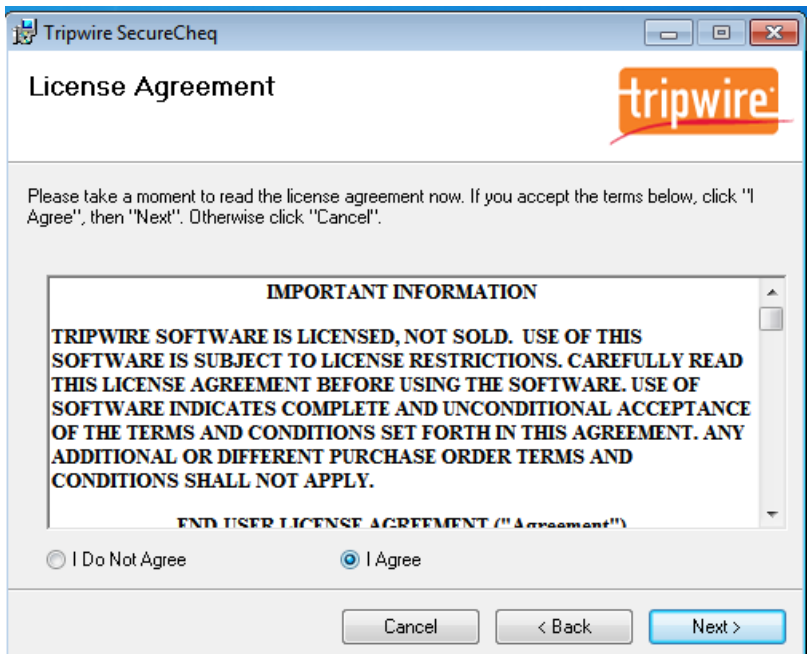


Installation (Step - 3)

- Click on “**Next**” to proceed the installation

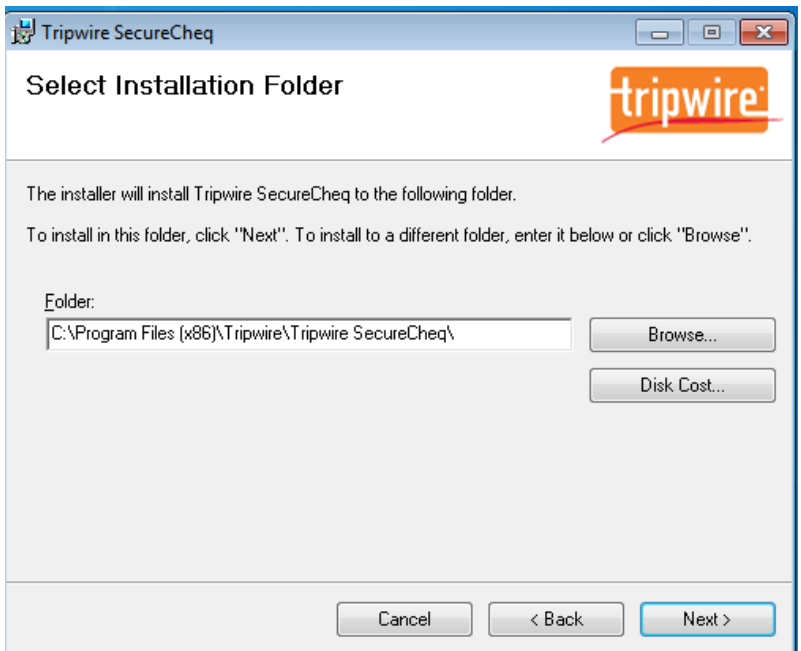
Installation (Step - 4)

- Read the Licence Agreement and select “**I Agree**”. Then click on “**Next**”.



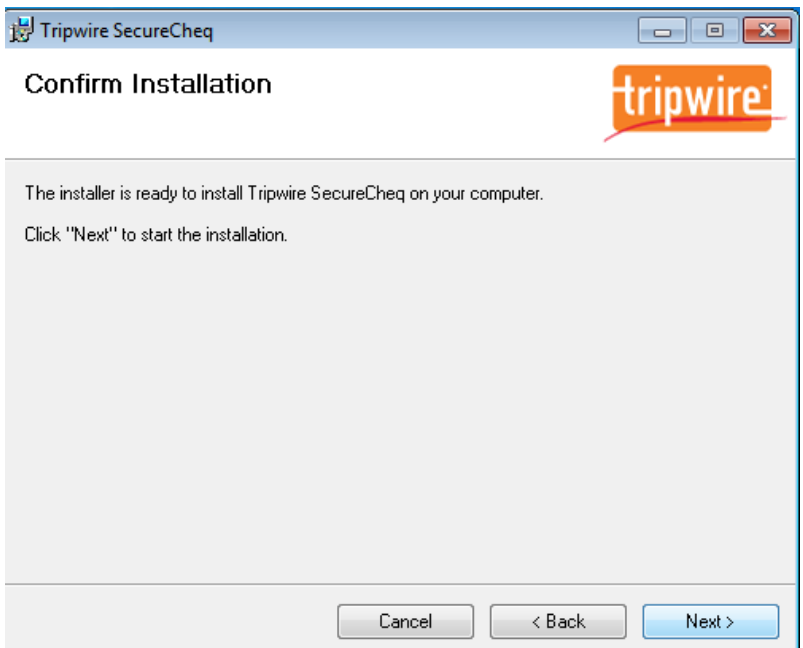
Installation (Step - 5)

- Choose installation folder. Then click on “**Next**”.



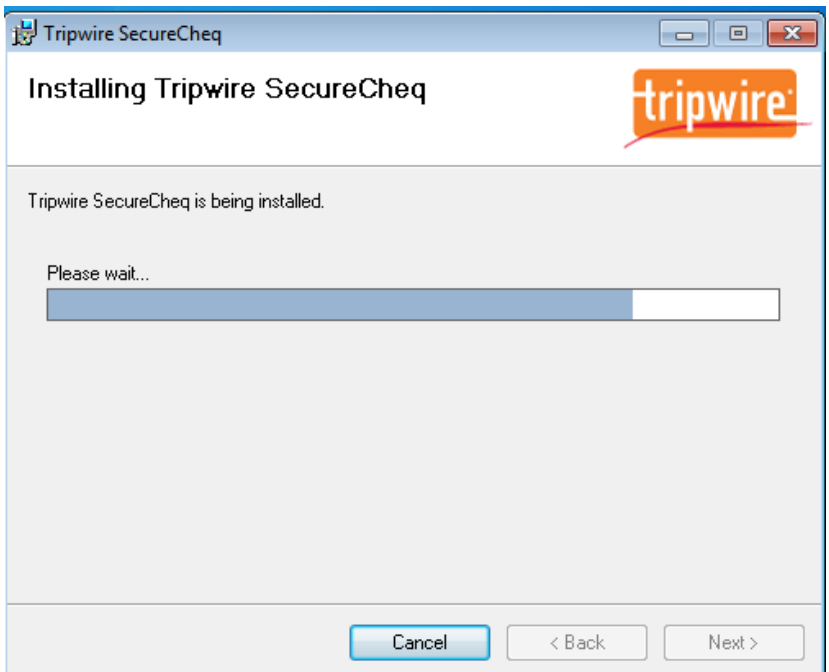
Installation (Step - 6)

- Click on “**Next**” to confirm installation



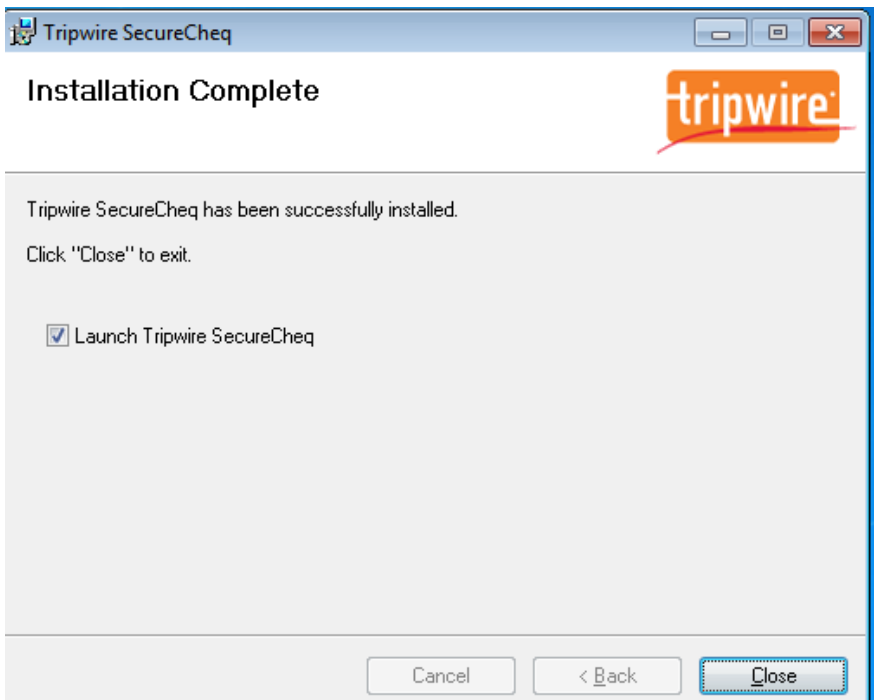
Installation (Step - 7)

- The progress bar will be display installation progress



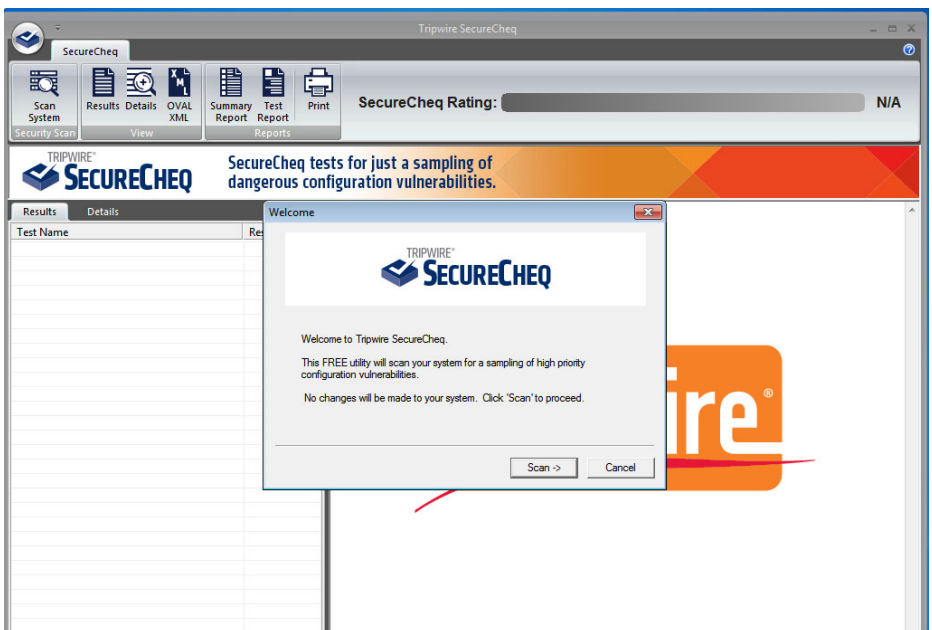
Installation (Step - 8)

- Now click on “**Close**” to complete the installation



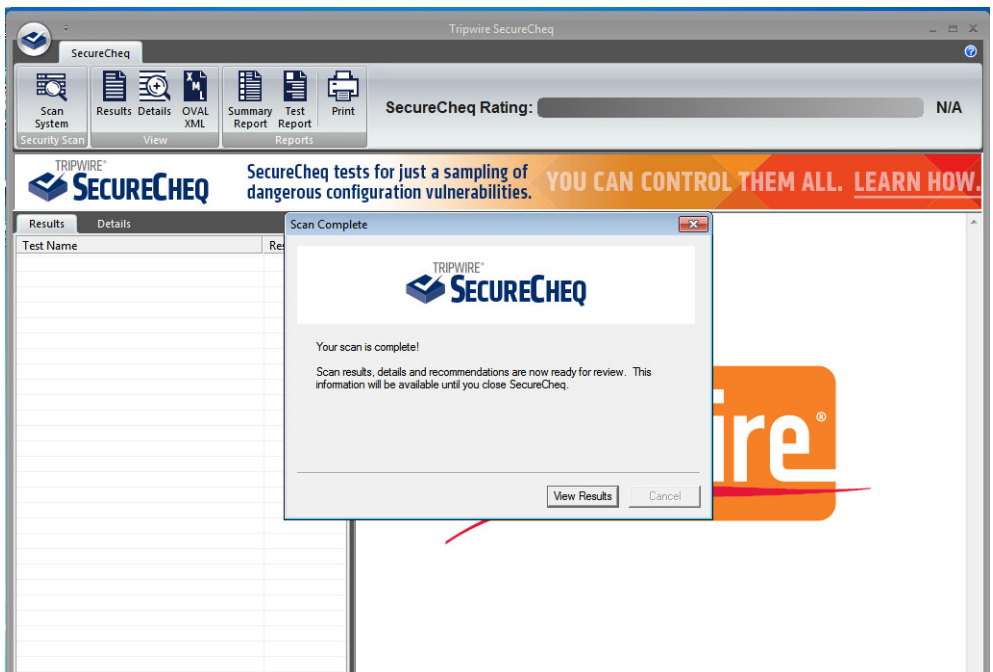
Starting the Scan (Step - 1)

- Now the Tripwire SecureCheq will start and will ask to scan the system. Click on "**Scan**" to beginning scanning the system



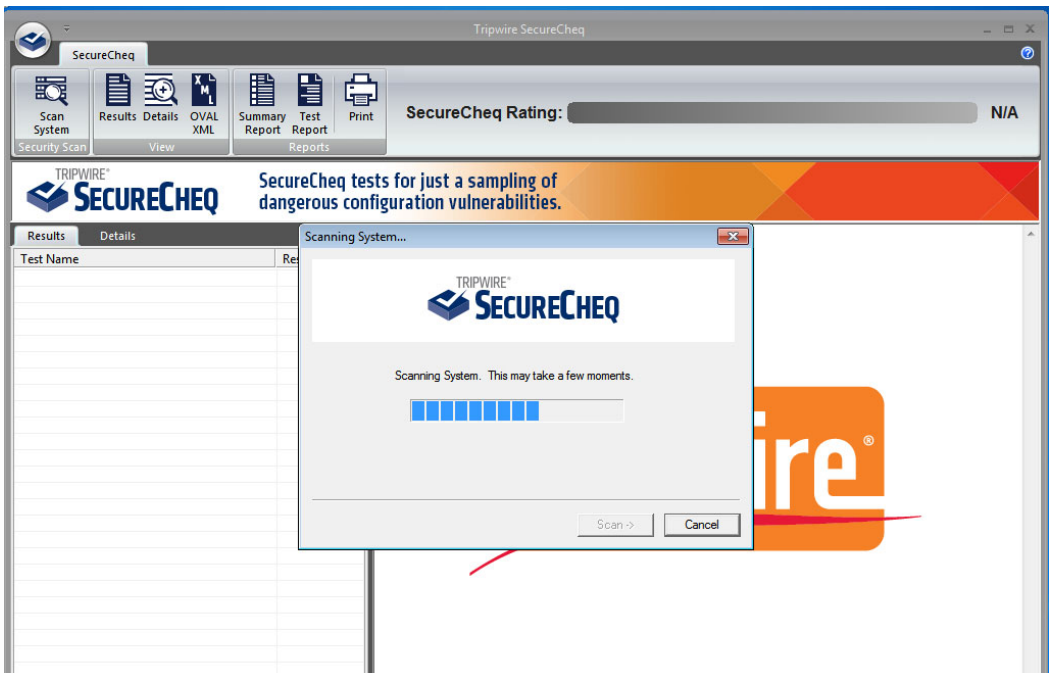
Starting the Scan (Step - 2)

- SecureCheq will now start scanning



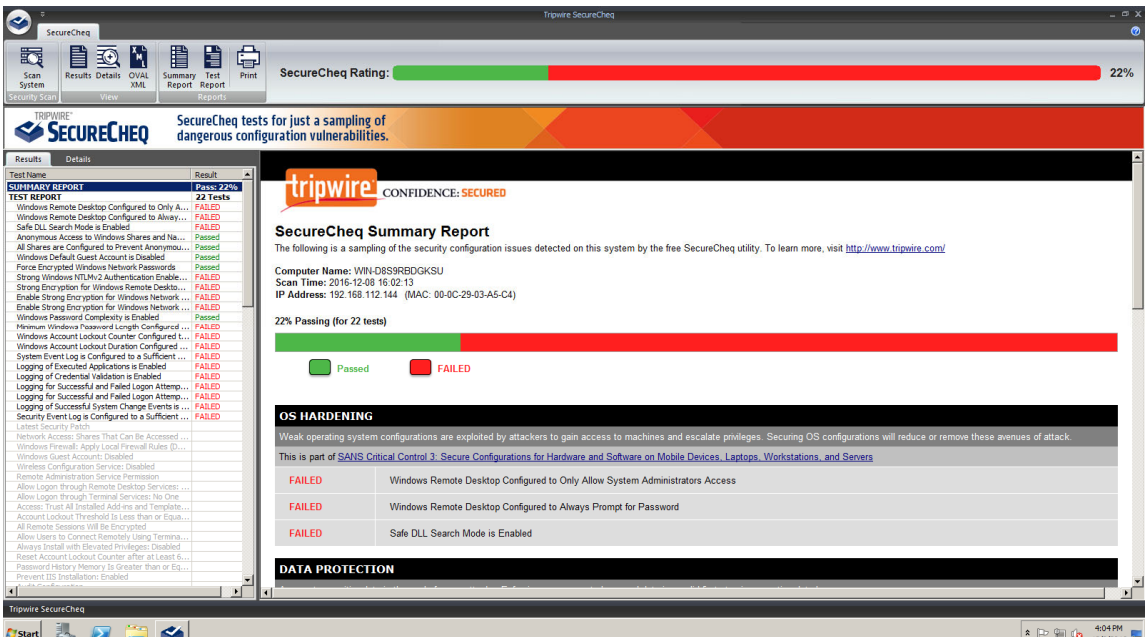
Starting the Scan (Step - 3)

- After the scan is complete, the results can be viewed by clicking on "**View Results**"

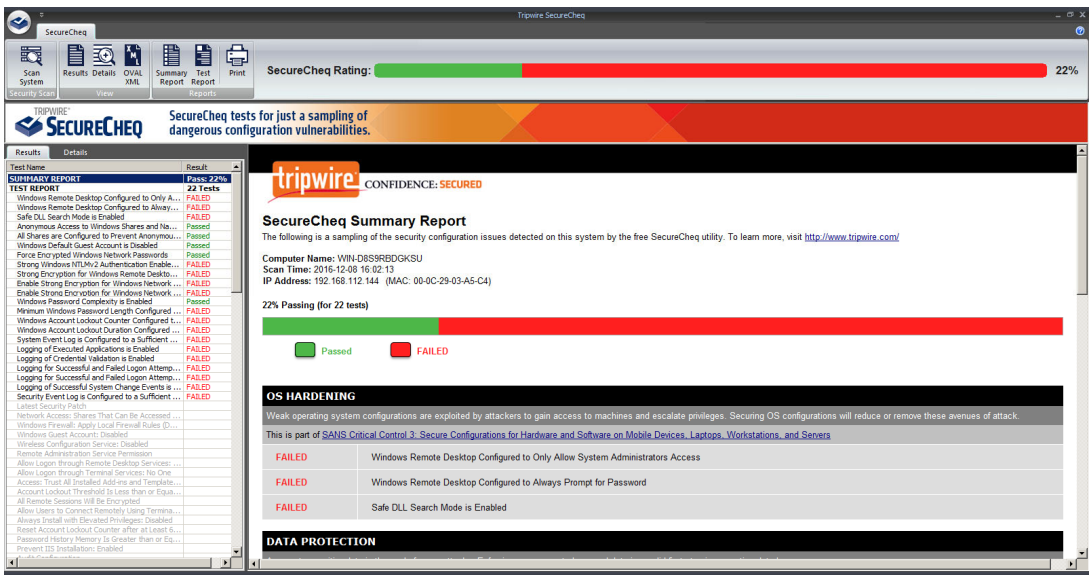


Starting the Scan (Step - 4)

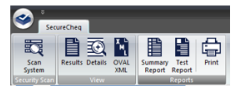
- Scan results will be displayed as “**SecureCheq Summary Report**”.



About the tool window



About the tool window



Security Scan: It consists of **Scan System** button. By clicking on this on this button, a fresh scan can be initiated.

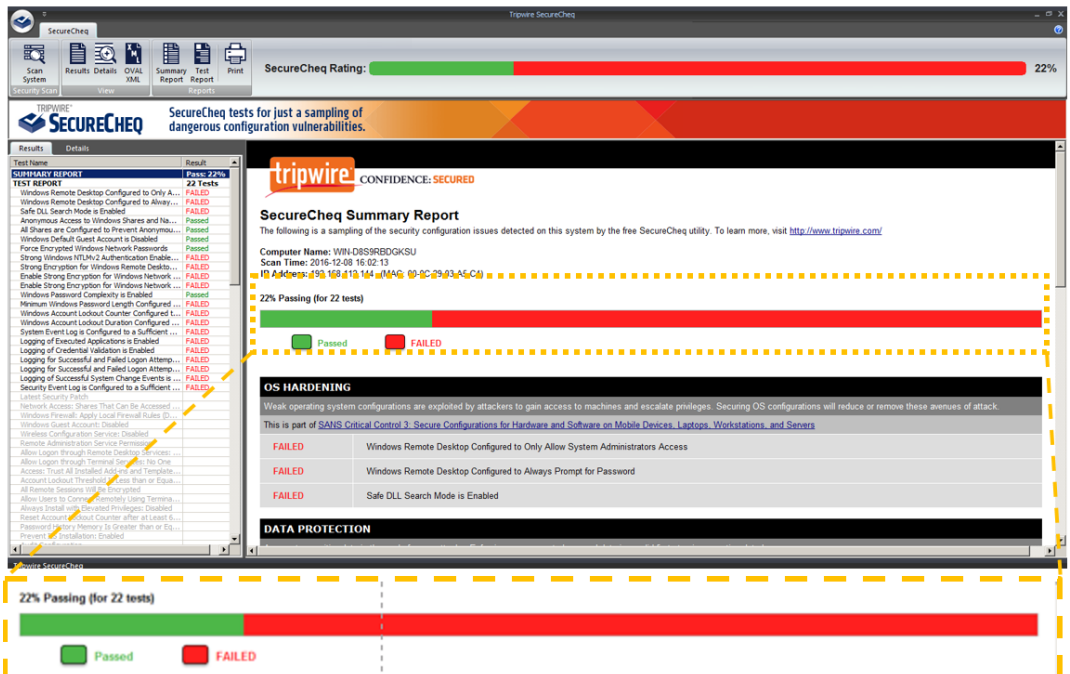
View: Following buttons are displayed in this pane:

1. **Results:** Shows results of the scan i.e. displays the scan report
2. **Details:** Details corresponding to each security issue are displayed after clicking on this button
3. **Oval XML:** Opens XML file in open vulnerability and assessment language (oval) containing information about the tests run

Report: Following buttons are displayed in this pane:

1. **Summary Report:** Shows broad categories of the security configuration issues detected
2. **Test Report:** Shows detailed report on each of the tests conducted with a background about the test conducted, the result of the test (Passed/Failed), the remediation techniques and references from internet for further study on the test and the issues
3. **Print:** Prints scan report

SecureCheq Summary Report



System aspects covered in scan

- OS Hardening

OS HARDENING	
Weak operating system configurations are exploited by attackers to gain access to machines and escalate privileges. Securing OS configurations will reduce or remove these avenues of attack.	
This is part of SANS Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	
FAILED	Windows Remote Desktop Configured to Only Allow System Administrators Access
FAILED	Windows Remote Desktop Configured to Always Prompt for Password
FAILED	Safe DLL Search Mode is Enabled

System aspects covered in scan

- Data Protection

DATA PROTECTION	
Access to sensitive data is the goal of many attacks. Enforcing access controls around data is a solid first step in preventing data loss.	
This is part of SANS Critical Control 15: Controlled Access Based on the Need to Know and SANS Critical Control 17: Data Loss Prevention	
Passed	Anonymous Access to Windows Shares and Named Pipes is Disallowed
Passed	All Shares are Configured to Prevent Anonymous Access
Passed	Windows Default Guest Account is Disabled

System aspects covered in scan

- Communication Security

COMMUNICATION SECURITY	
Access to sensitive information such as user credentials, credit card information, and intellectual property is a common objective of many attackers.	
Encrypting transmissions of this information makes it less susceptible to interception by attackers, and is an underpinning of many security controls and standards.	
Passed	Force Encrypted Windows Network Passwords
FAILED	Strong Windows NTLMv2 Authentication Enabled; Weak LM Disabled
FAILED	Strong Encryption for Windows Remote Desktop Required
FAILED	Enable Strong Encryption for Windows Network Sessions on Clients
FAILED	Enable Strong Encryption for Windows Network Sessions on Servers

System aspects covered in scan

- User Account Security

USER ACCOUNT SECURITY	
Legitimate user accounts are often exploited by attackers to gain access to sensitive systems and hide their tracks. Strengthening user account security helps protect against these attacks.	
This is part of SANS Critical Control 16: Account Monitoring and Control and many other security frameworks.	
Passed	Windows Password Complexity is Enabled
FAILED	Minimum Windows Password Length Configured to be at Least 8 Characters
FAILED	Windows Account Lockout Counter Configured to Wait at Least 15 Minutes Before Reset
FAILED	Windows Account Lockout Duration Configured to at Least 15 Minutes

System aspects covered in scan

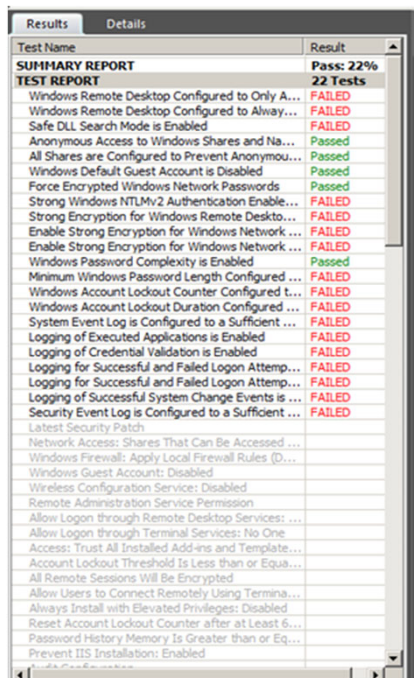
- Log and Auditing

LOGS AND AUDITING	
Lack of adequate security logging allows hackers to hide their activities on compromised machines, while intentional disabling of security logs is often the first stage of an attack.	
Continuously logging is part of SANS Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs and a widely accepted best practice.	
FAILED	System Event Log is Configured to a Sufficient Size
FAILED	Logging of Executed Applications is Enabled
FAILED	Logging of Credential Validation is Enabled
FAILED	Logging for Successful and Failed Logon Attempts for Domain Accounts is Enabled
FAILED	Logging for Successful and Failed Logon Attempts for Local Accounts is Enabled
FAILED	Logging of Successful System Change Events is Enabled
FAILED	Security Event Log is Configured to a Sufficient Size

SecureCheq Test Report

- Tests Conducted

SecureCheq Test Report

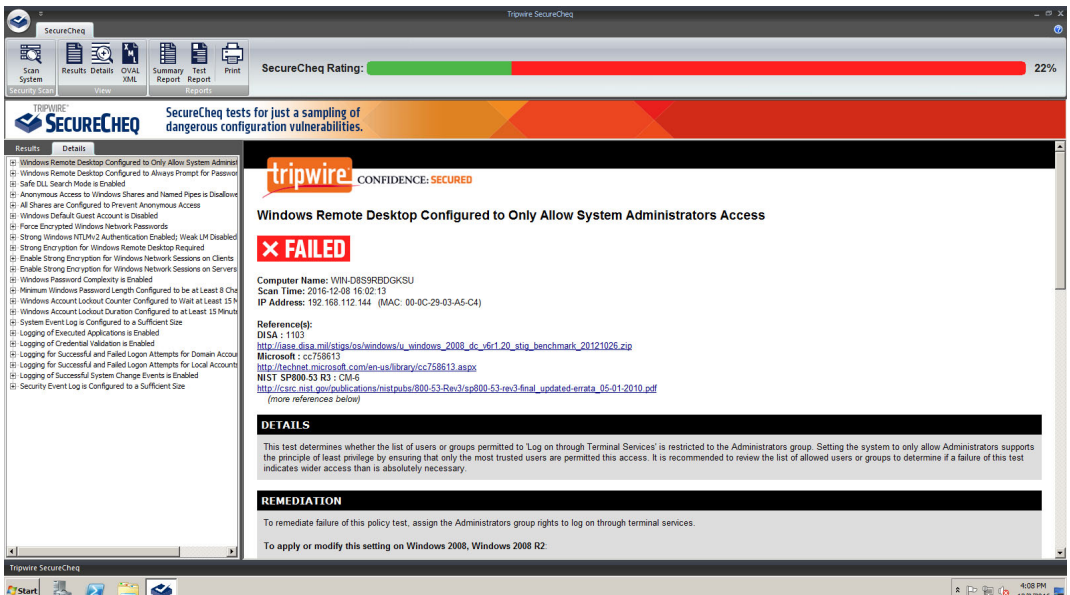


Results | Details

Test Name	Result
SUMMARY REPORT	**Pass: 22%**
TEST REPORT	**22 Tests**
Windows Remote Desktop Configured to Only A...	FAILED
Windows Remote Desktop Configured to Alway...	FAILED
Safe DLL Search Mode is Enabled	FAILED
Anonymous Access to Windows Shares and Na...	Passed
All Shares are Configured to Prevent Anonymou...	Passed
Windows Default Guest Account is Disabled	Passed
Force Encrypted Windows Network Passwords	Passed
Strong Windows NTLMv2 Authentication Enable...	FAILED
Strong Encryption for Windows Remote Deskto...	FAILED
Enable Strong Encryption for Windows Network ...	FAILED
Enable Strong Encryption for Windows Network ...	FAILED
Windows Password Complexity is Enabled	Passed
Minimum Windows Password Length Configured ...	FAILED
Windows Account Lockout Counter Configured t...	FAILED
Windows Account Lockout Duration Configured ...	FAILED
System Event Log is Configured to a Sufficient ...	FAILED
Logging of Executed Applications is Enabled	FAILED
Logging of Credential Validation is Enabled	FAILED
Logging for Successful and Failed Logon Attemp...	FAILED
Logging for Successful and Failed Logon Attemp...	FAILED
Logging of Successful System Change Events is ...	FAILED
Security Event Log is Configured to a Sufficient ...	FAILED
Latest Security Patch	
Network Access: Shares That Can Be Accessed ...	
Windows Firewall: Apply Local Firewall Rules (D...	
Windows Guest Account: Disabled	
Wireless Configuration Service: Disabled	
Remote Administration Service Permission	
Allow Logon through Remote Desktop Services: ...	
Allow Logon through Terminal Services: No One	
Access: Trust All Installed Add-ins and Template...	
Account Lockout Threshold Is Less than or Equa...	
All Remote Sessions Will Be Encrypted	
Allow Users to Connect Remotely Using Termina...	
Always Install with Elevated Privileges: Disabled	
Reset Account Lockout Counter after at Least 6...	
Password History Memory Is Greater than or Eq...	
Prevent IIS Installation: Enabled	

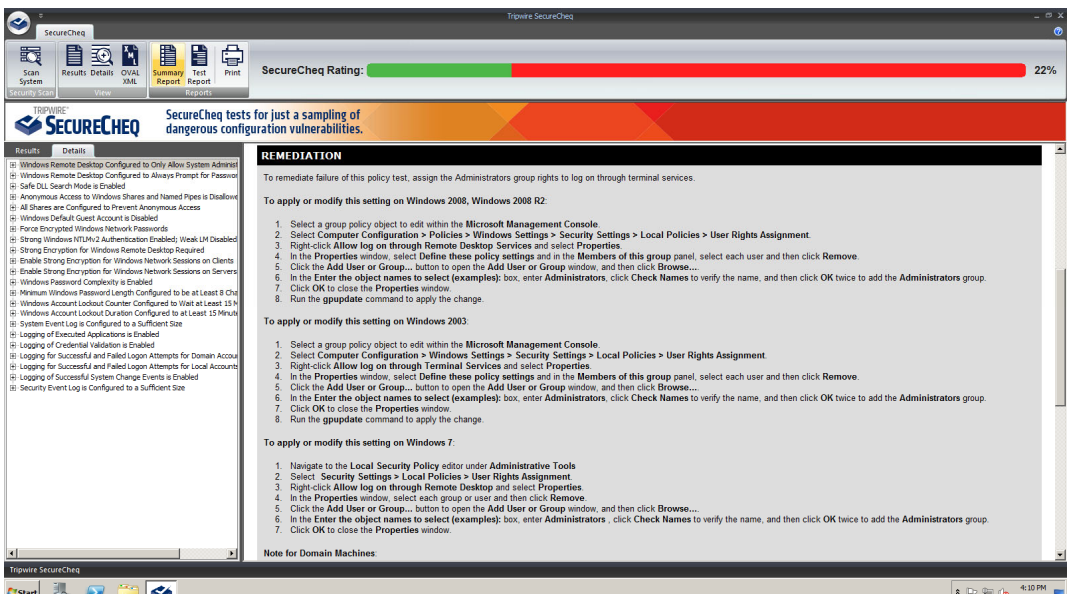
SecureCheq Test Report

- Windows Remote Desktop Configured to Only Allow System Administrators Access



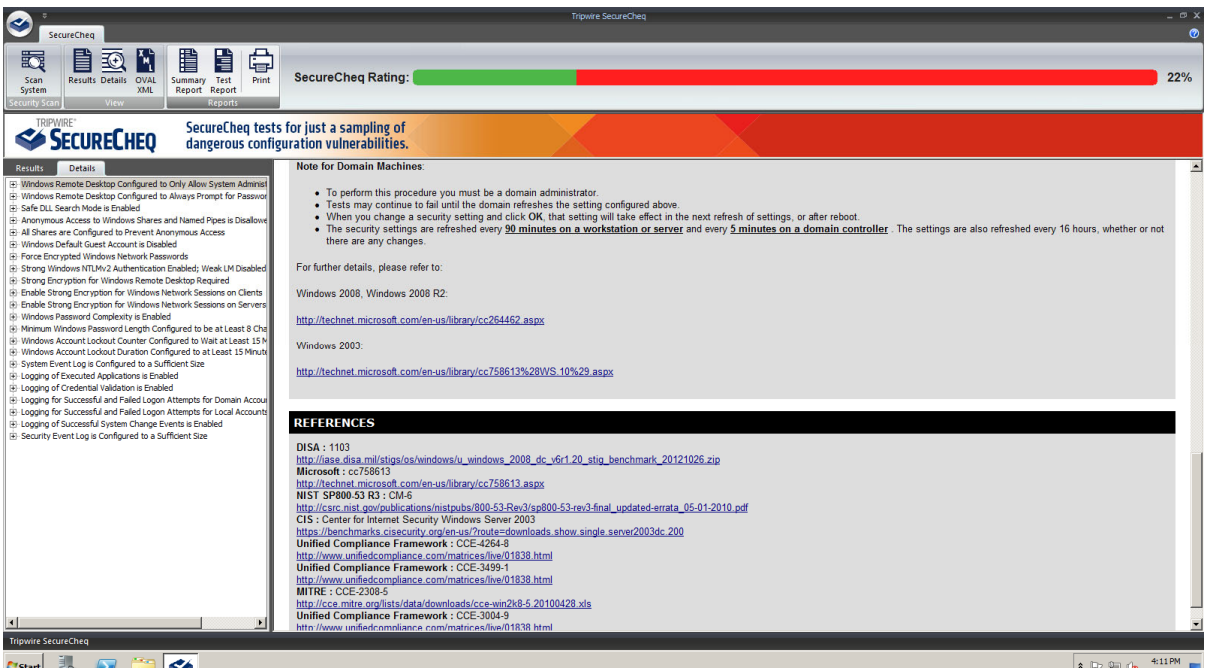
SecureCheq Test Report

- Windows Remote Desktop Configured to Only Allow System Administrators Access



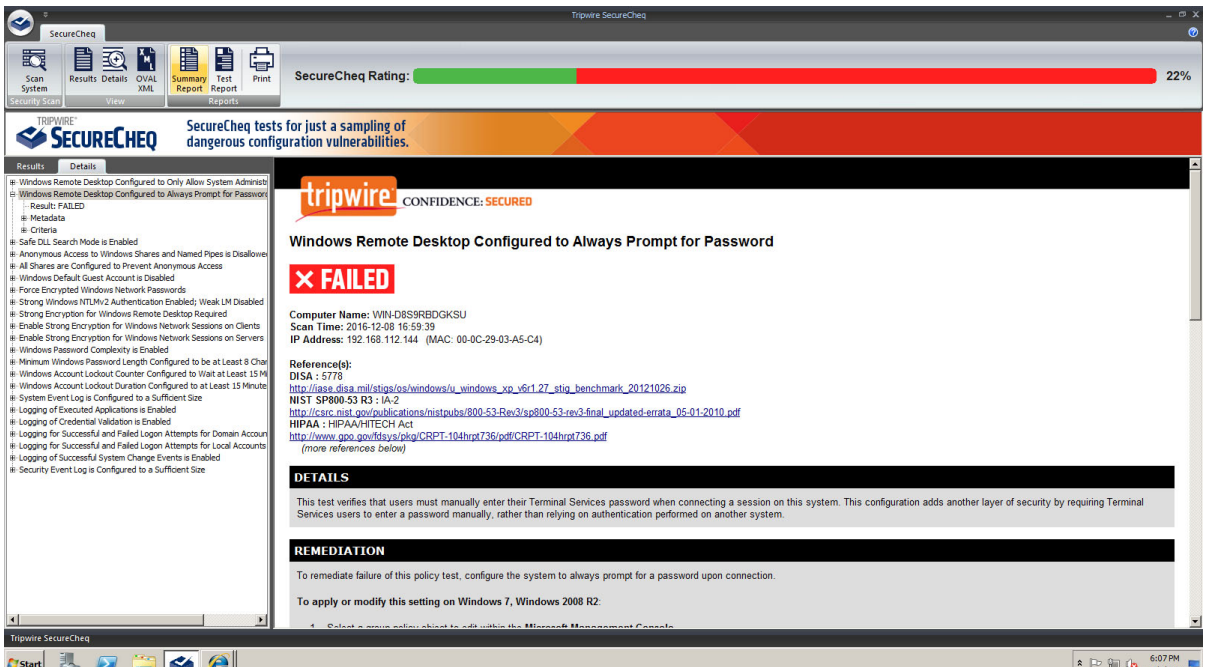
SecureCheq Test Report

- Windows Remote Desktop Configured to Only Allow System Administrators Access



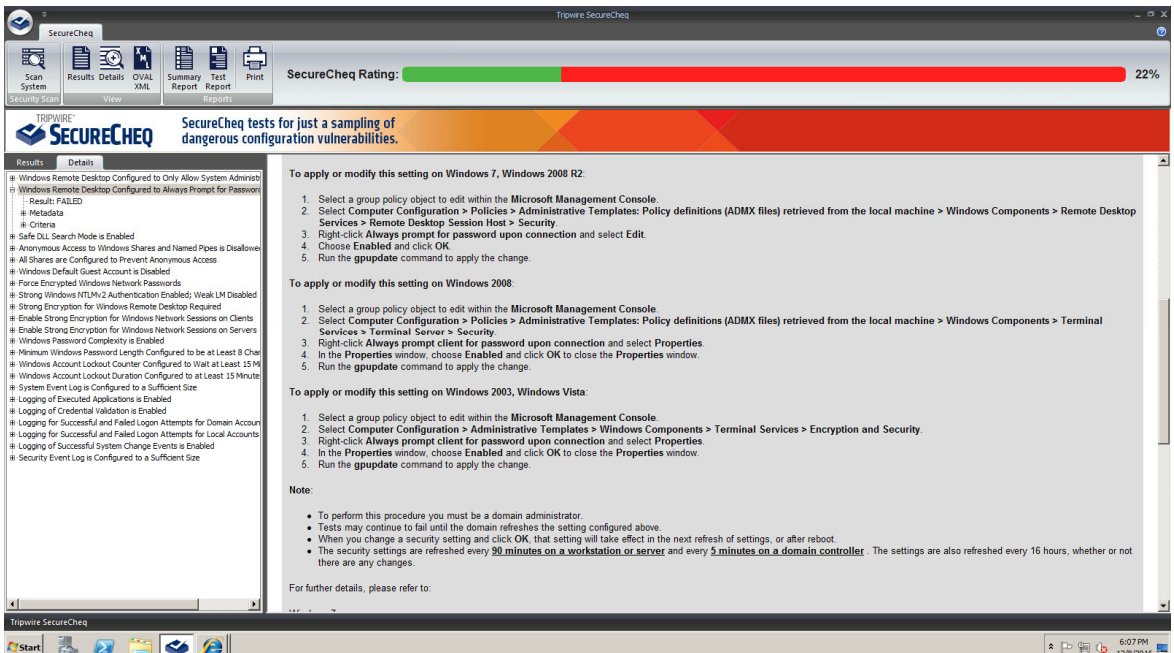
SecureCheq Test Report

- Windows Remote Desktop Configured to Always Prompt for Password



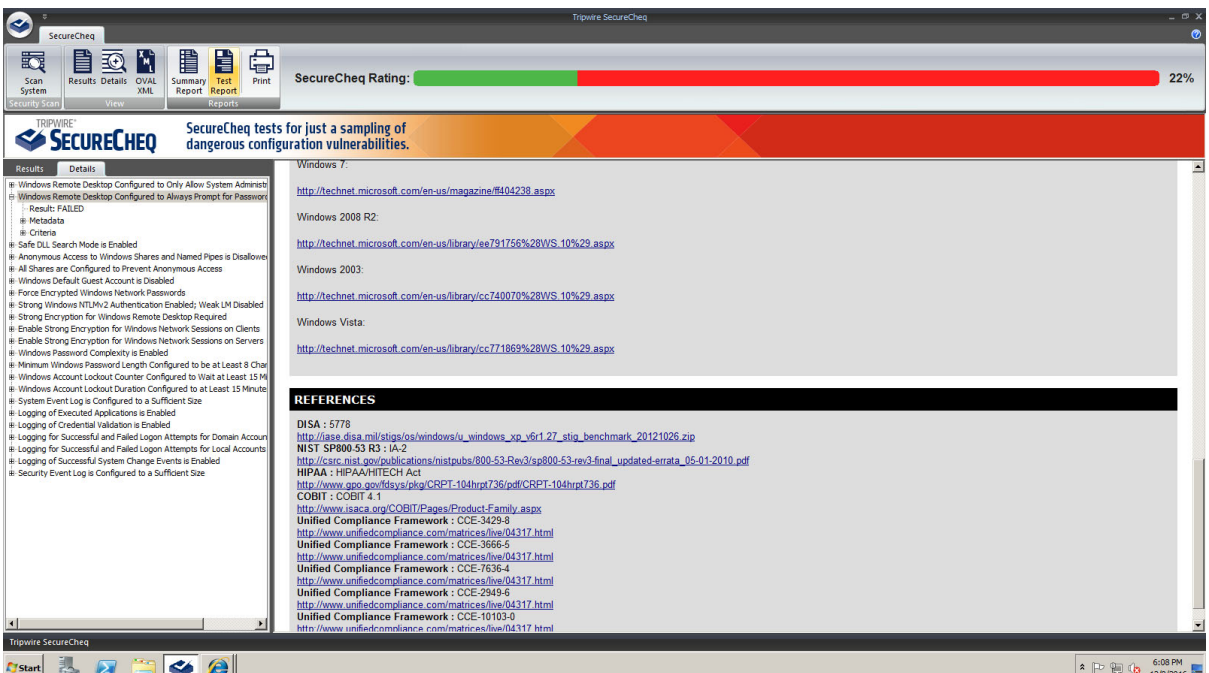
SecureCheq Test Report

- Windows Remote Desktop Configured to Always Prompt for Password



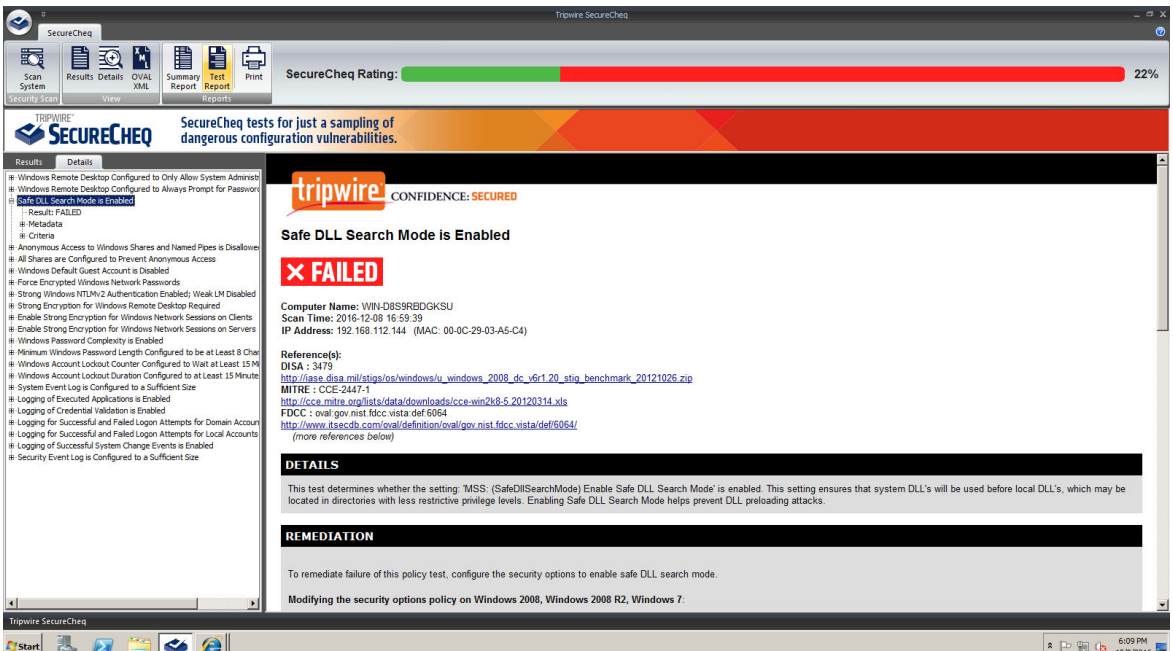
SecureCheq Test Report

- Windows Remote Desktop Configured to Always Prompt for Password



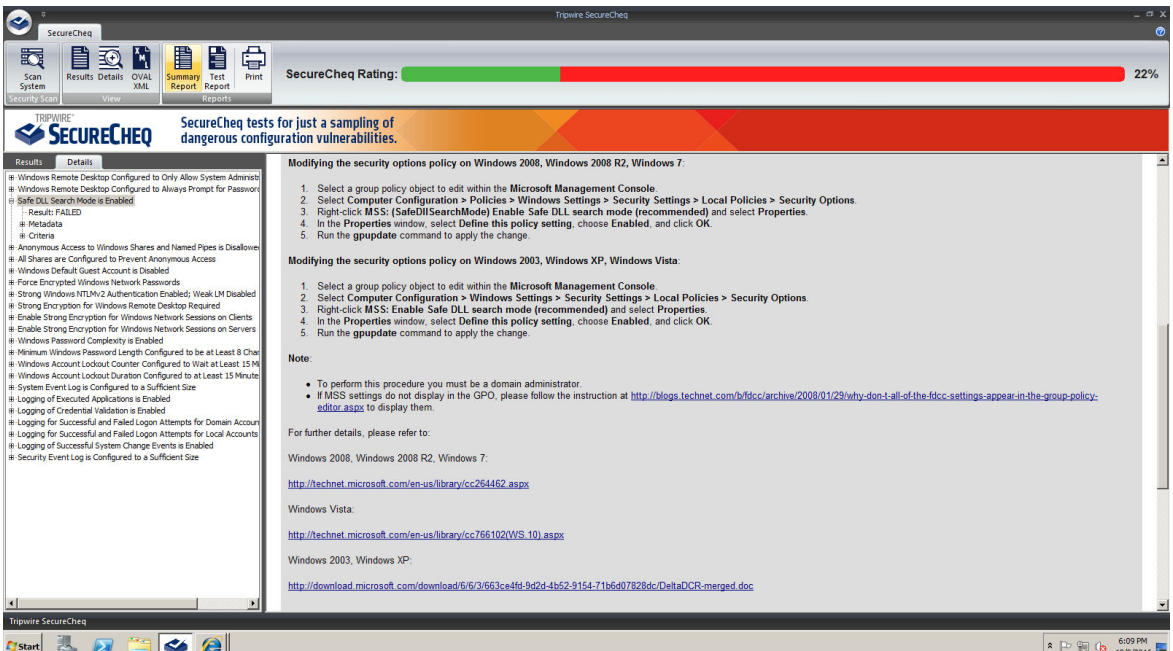
SecureCheq Test Report

- Safe DLL Search Mode is Enabled



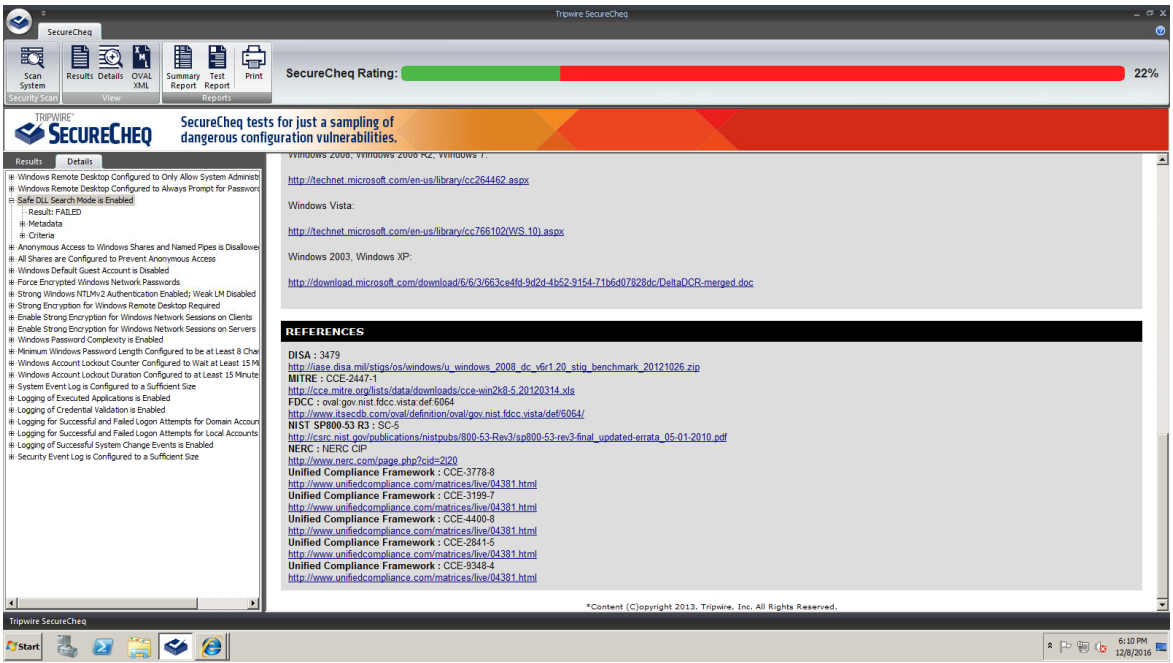
SecureCheq Test Report

- Safe DLL Search Mode is Enabled



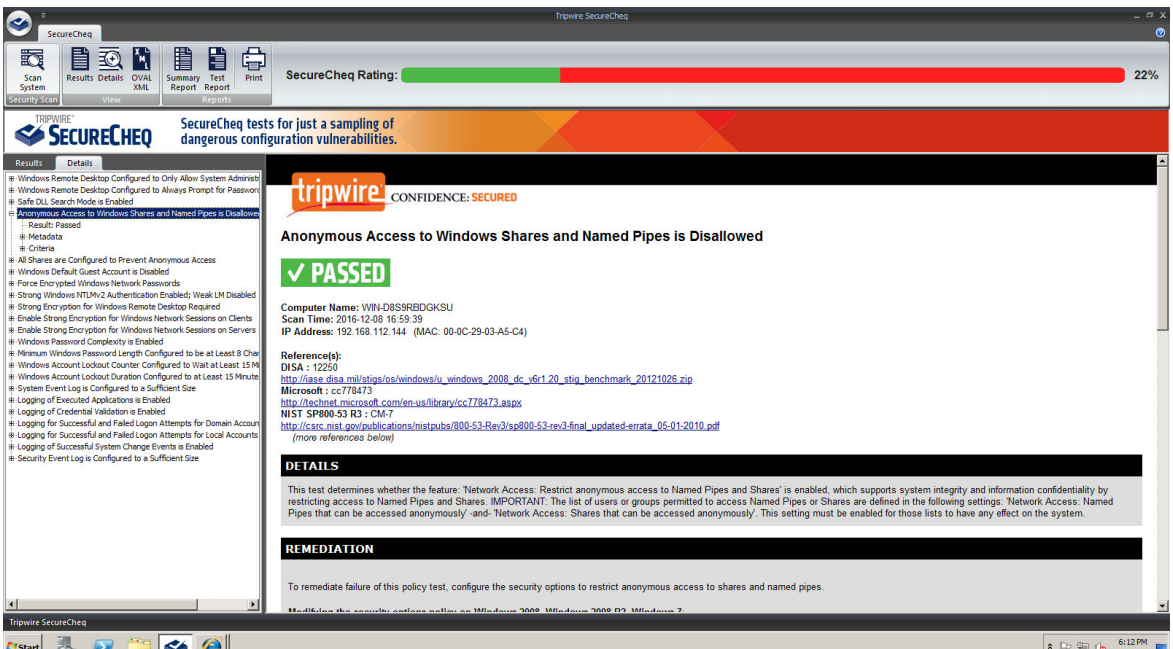
SecureCheq Test Report

- Safe DLL Search Mode is Enabled



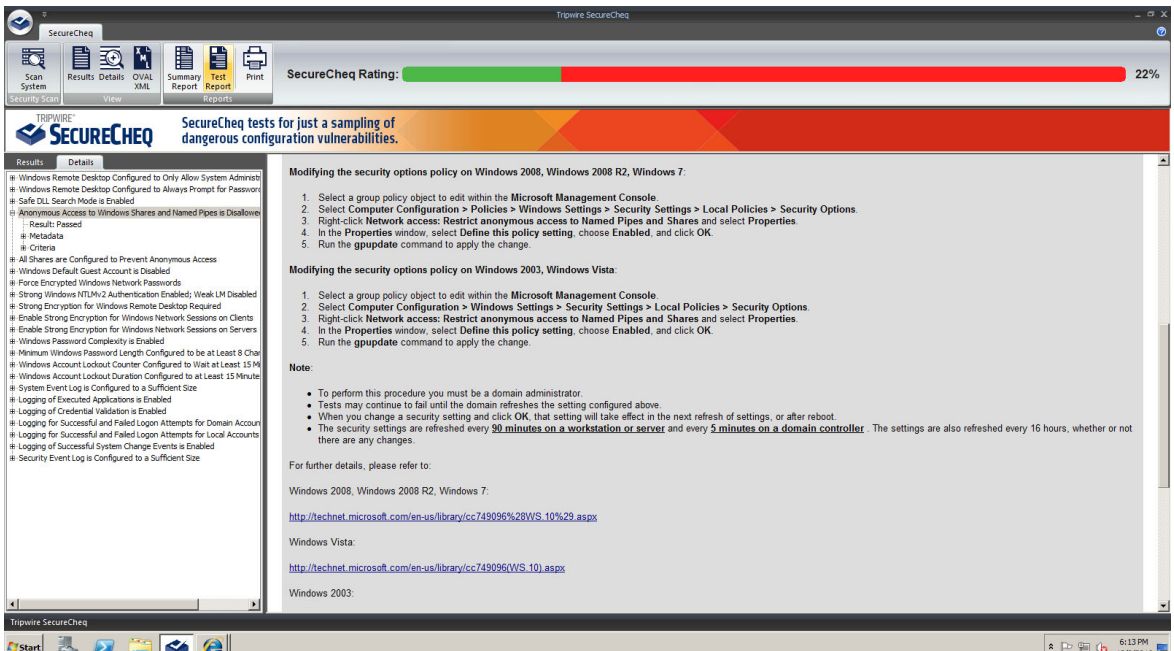
SecureCheq Test Report

- Anonymous Access to Windows Shares and Named Pipes is Disallowed



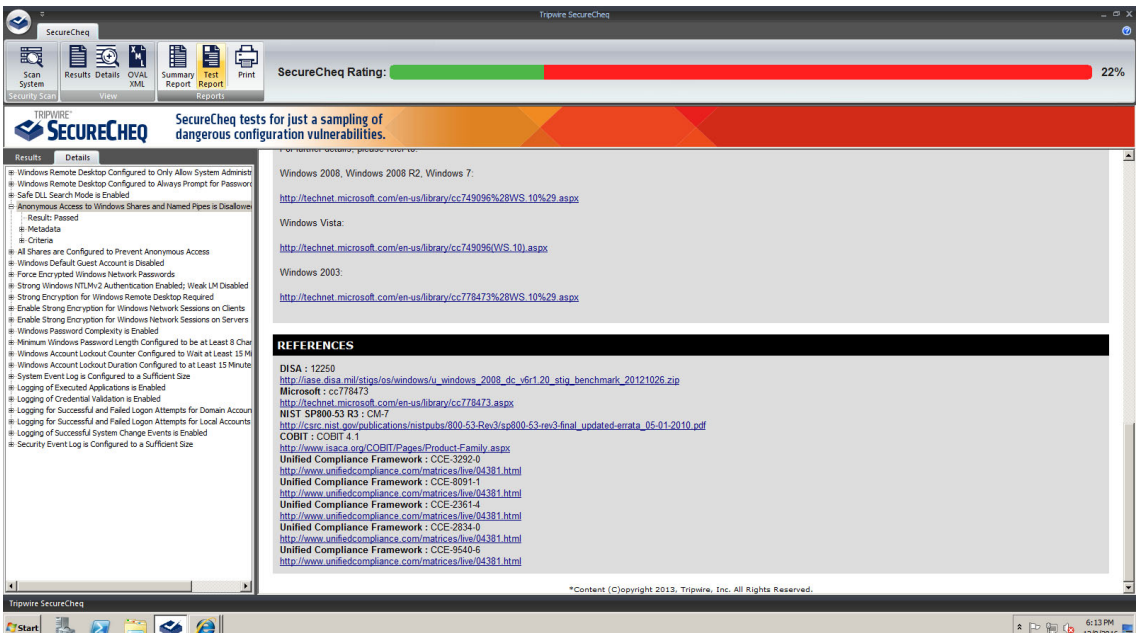
SecureCheq Test Report

- Anonymous Access to Windows Shares and Named Pipes is Disallowed



SecureCheq Test Report

- Anonymous Access to Windows Shares and Named Pipes is Disallowed



Checkpoint

1. How is UNIX protection system a discretionary access control system
   A. It checks whether the process identity's UID corresponds to the owner UID of the file being accessed
   B. owner UID, or group GID may be changed by any UNIX processes run by the file's owner, that have the same UID as the file owner
   C. owner UID is never allowed to be changed
   D. none of the above
2. What security mechanism is followed by Microsoft Windows' Applocker?
   A. Grant access to file based upon the attributes of file and identity of user
   B. Mark application data as non-executable
   C. Decrypt all the application and user data
   D. Use a tamper-proof hardware chip (Trusted Platform Module) which stores encryption key material
3. Which of the following is true about Network Access Protection?
   A. It is assured that the operating system is not compromised before it gets access to a corporate network
   B. Limit the number of external connections to allow successful connections to be made only to trusted resources
   C. Limit access to objects in its operating systems
   D. All of the above

Checkpoint

4. How do modern operating systems judge the code to be executed?
   A. By matching the fingerprint or “hash” of the application to be executed with the cryptographically signed hash
   B. Virtualize whole operating system and run on a hypervisor
   C. Code is marked executable or non-executable
   D. Use a Trusted Platform Module
5. What happens in Time-of-Check-to-Time-of-Use (TOCTTOU) attacks?
   A. The state of the system between the time an operation is authorized and the time that the operation is performed is changed
   B. The identity of the user (attacker? between the time an operation is authorized and the time that the operation is performed is changed
   C. The code being executed between the time an operation is authorized and the time that the operation is performed is changed
   D. None of the above
6. What purpose do Service Packs serve in securing server operating system?
   A. They are installed and used in managing patches to fix security vulnerabilities that are well known to intruders
   B. Ensure that only required network services should be installed in the server
   C. They are not a security solution but a threat
   D. Both A and B

Checkpoint

7. Which one of the following is not true for hardening operating systems?
   A. Boot on “OS banner” should be enabled
   B. OS media should be procured only from an authorised vendor of the manufacturer
   C. Turn off all network services that are not needed
   D. All of the above are true
8. Which layer in Apple iOS Layer constitutes the section that enables using Audio, Animation video and Image formats (JPEG, PNG, TIFF) and documents?
   A. Media Layer
   B. A layer in Cocoa Touch platform
   C. Core Services layer
   D. Both A and B
9. Which Mobile OS threat can penetrate the existing documents and send them elsewhere?
   A. Trojan
   B. Worm
   C. Virus
   D. Spyware

Checkpoint

10. How are Denial of Service attacks directed in mobile devices?
    A. Through applications or malware installed in smartphones
    B. Using the vulnerabilities created by the malformed text messages. In addition to these attack vectors
    C. Directing the user to the imitation websites instead of the legitimate ones in order to steal their private information
    D. Both A and C

Checkpoint solutions

1. B
2. A
3. A
4. A
5. A
6. A
7. A
8. D
9. A
10. B

Unit summary

Having completed this unit, you should be able to:

- Get to know the threats that are faced by operating systems and how they are evolving
- Understand key security features of operating systems
- Get an insight on the security guidelines for server and workstation operating systems
- Get familiar with threats in various mobile operating systems

Endpoint Security

Unit objectives

After completing this unit, you should be able to:

- Know what are the threats that drive the need of endpoint security solutions
- Get familiar with the components with endpoint security
- Understand the challenges faced by endpoint security
- Relate the deployment of endpoint security solutions with practical scenarios

What is Endpoint Security?

- Introduction of Endpoint security
  - Critical Components of Endpoint Security
  - Endpoint security perspectives: Consumer versus corporate

Pillars of Endpoint Security

- Four Pillars of Endpoint Security
  - Endpoint Hardening
  - Endpoint Resiliency
  - Network Prioritization
  - Network Resiliency

Endpoint Security in BYOD

- Four Pillars of Endpoint Security in Bring your own device (BYOD)
  - Endpoint Hardening
  - Endpoint Reliability
  - Network Prioritization
  - Network Resiliency

Endpoint Encryption

- Defining endpoint encryption and its difference modes
  - Disk Encryption
  - Removable Media Encryption

Driver influence endpoint security

- Explaining the business drivers that influence the endpoint security
  - Correct and reliable operation
  - Service-level agreements
  - IT asset value
  - Protection of the business asset value or brand image
  - Legal and regulatory compliance
  - Contractual obligation
  - Financial loss and liability
  - Critical infrastructure
  - Safety and survival

Driver influence endpoint security

- Explaining the IT drivers that influence the endpoint security
  - Internal threats and threat agents
  - External threats and threat agents
  - IT service management commitments
  - IT environment complexity
  - Business environment complexity
  - Audit and traceability
  - IT vulnerabilities: Configuration
  - IT vulnerabilities: Flaws
  - IT vulnerabilities: Exploits
  - End User Complexity
  - Fast-Growing Web Threats
  - VPN Security Challenges

Challenges of Endpoint Security (1 of 2)

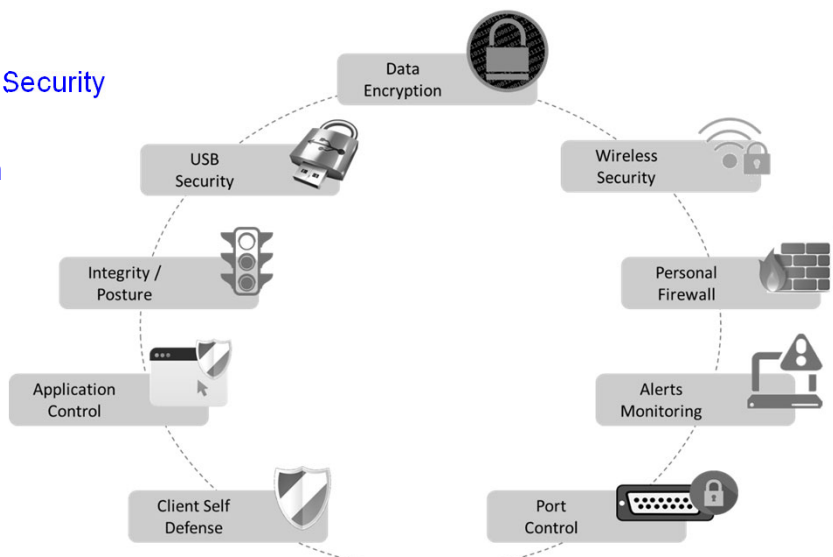
- Some major challenges while delivering endpoint security
  - Complacency and Risk
  - Business Challenges
  - The Threats Keep Coming

Challenges of Endpoint Security (2 of 2)

- Some major challenges while delivering endpoint security
  - Protecting Mobile Users
  - Client-side Performance
  - Overworked IT Staff
  - The Cloud Alternative

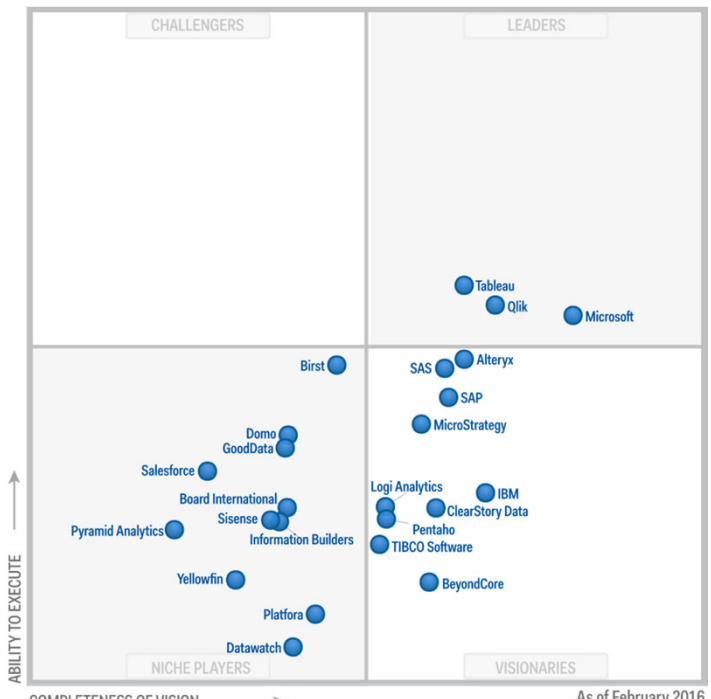
Endpoint Security Solutions

- General aspects covered by an Endpoint Solution
  - Personal Firewall
  - Wireless Security
  - Port Control
  - Data Encryption
  - USB and Storage Device Security
  - Application Control
  - Integrity and Remediation
  - Client Self-Defense
  - Alerts Monitoring



Gartner's Magic Quadrant

- Endpoint protection platforms capabilities & things include in EPP
  - Antimalware
  - Personal firewall
  - Port and device control



Quadrant Descriptions

- Explaining the quadrant descriptions
  - Leaders
  - Challengers
  - Visionaries
  - Niche Players

Evaluation Criteria Definitions

- Explaining the evaluation criteria definitions
  - Ability to Execute
  - Vendor Strengths and Limitations

Vendor Strengths and Limitations (1 of 6)

- Defining Vendor Strengths and Limitations
  - Bitdefender
  - Check Point Software Technologies
  - Cylance

Vendor Strengths and Limitations (2 of 6)

- Defining Vendor Strengths and Limitations
  - Eset
  - FSecure
  - Heat Software

Vendor Strengths and Limitations (3 of 6)

- Defining Vendor Strengths and Limitations
  - IBM
  - Intel Security
  - Kaspersky Lab

Vendor Strengths and Limitations (4 of 6)

- Defining Vendor Strengths and Limitations
  - Landesk
  - Microsoft
  - Panda Security

Vendor Strengths and Limitations (5 of 6)

- Defining Vendor Strengths and Limitations
  - Qihoo 360
  - SentinelOne
  - Sophos

Vendor Strengths and Limitations (6 of 6)

- Defining Vendor Strengths and Limitations
  - Trend Micro
  - Webroot

Case Study 1: Palo Alto Networks

- Let’s solve the case study on Palo Alto Networks
  - Challenge
  - Solution
  - Results
  - Summary
  - Putting an End to Endpoint Attacks
  - Cybersecurity from End to End
  - Seeing Is Believing
  - Uniform Control and Prevention
  - Secure Infrastructure Means Secure Business

Case Study 2: Trend Micro

- Let's solve the case study on Tread Micro
  - Challenge: Security Causing Performance
  - Solution: Agentless Security Drives Down CapEx and OpEx
  - Effective Protection at the Hypervisor Level
  - Immediate Protection in the Cloud
  - Results: Business Continuity Along with Efficiency Gains

Checkpoint

1. Which of the following is true for Disk Encryption?
   A. Disk encryption modifies the boot sector
   B. Disk encryption typically uses one key to encrypt a hard disk
   C. Disk encryption protects a hard drive in the event of theft or accidental loss by encrypting the entire disk
   D. All of the above
2. How is network resiliency similar to endpoint resiliency?
   A. Both facilitate network self-healing in order to minimize the management burden
   B. Both ensure that health information on devices and applications is continuously gathered and monitored
   C. They more or less represent the same thing
   D. They are not at all similar
3. Which attack redirects users to malicious sites owned by the attacker?
   A. Nine Ball
   B. Gumblar
   C. Lobo
   D. Deez Nuts

Checkpoint

4. Which attack works by infecting a legitimate Web site first and then redirecting visiting victim to a malicious site owned by the attacker?
   A. Deez Nuts
   B. Gumblar
   C. RiteWay
   D. None of the above
5. Which aspect of an endpoint solution secures all the endpoint communication ports and adapters?
   A. Port control
   B. Wireless fecurity
   C. Application control
   D. Personal firewall
6. Which one of the following statements is false?
   A. Bitdefender does not offer full feature parity between Windows, OS X and Linux
   B. The management console Cylance is cloud based
   C. Secure business solutions are targeted for SMBs seeking costeffective solutions with low administration overhead
   D. All are true

Checkpoint

7. Which business driver applies to circumstances where security threats and threat agents can affect the ability of an organization to conduct business?
   A. Contractual obligation
   B. Legal and regulatory compliance
   C. Service-level agreements
   D. IT asset value
8. Single points of failure for one or more business or management processes that are outside the enterprise boundary are an example of
   A. External threats
   B. Internal threats
   C. IT service management commitments
   D. None of the above
9. Which business challenge makes it harder to ensure that software installations and PC configurations are consistent?
   A. Ad-hoc PC management
   B. No in-house expertise
   C. Lack of IT resources
   D. None of the above

Checkpoint

10. Which of the following statemen(s) is true about cloud services?
    A. It requires little or no on-site hardware and companies usually pay for it on a per-user fee
    B. Streamlined management and ease of deployment
    C. Cloud security provider's data center is much more likely to possess the latest technology, high-end servers and fast connections
    D. All of the above

Checkpoint solutions

1. D
2. A
3. A
4. D
5. A
6. D
7. C
8. A
9. A
10. D

Unit summary

Having completed this unit, you should be able to:

- Know what are the threats that drive the need of endpoint security solutions
- Get familiar with the components with endpoint security
- Understand the challenges faced by endpoint security
- Relate the deployment of endpoint security solutions with practical scenarios

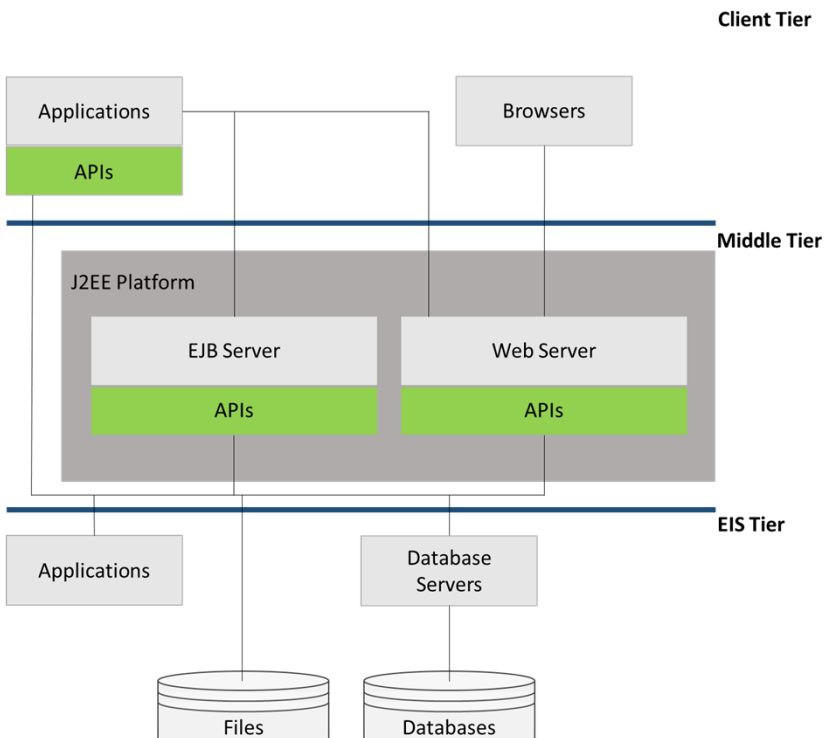
Application Server Security

Unit objectives

After completing this unit, you should be able to:

- Get acquainted with various application server threats and countermeasures
- Get an overview of general application server security overview
- Get familiar with the Oracle application server security architecture
- Understand the need of application server security

Application Server Security Overview

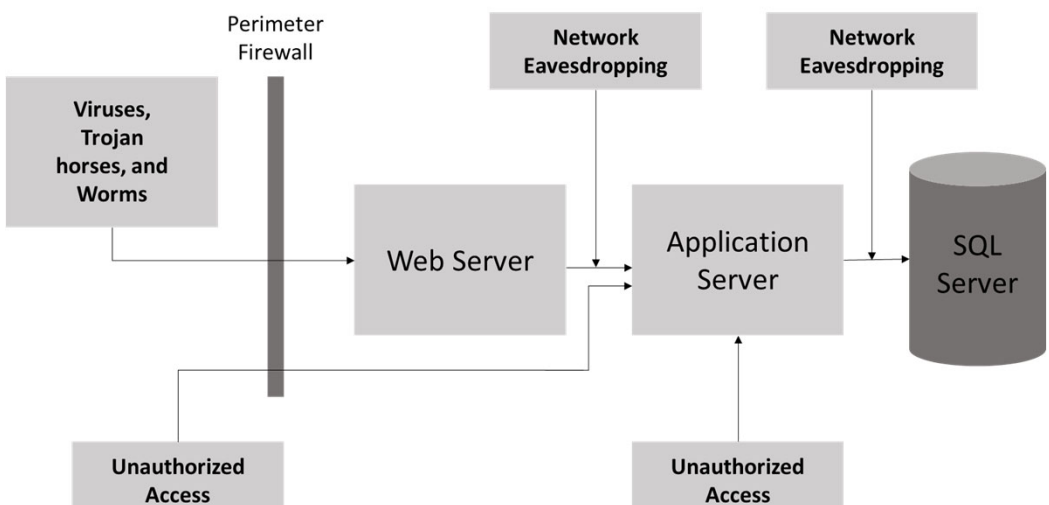


SSL Keys and Certificates

- Introduction to SSL Keys and Certificates
  - Steps to negotiated SSL session

Need of Security

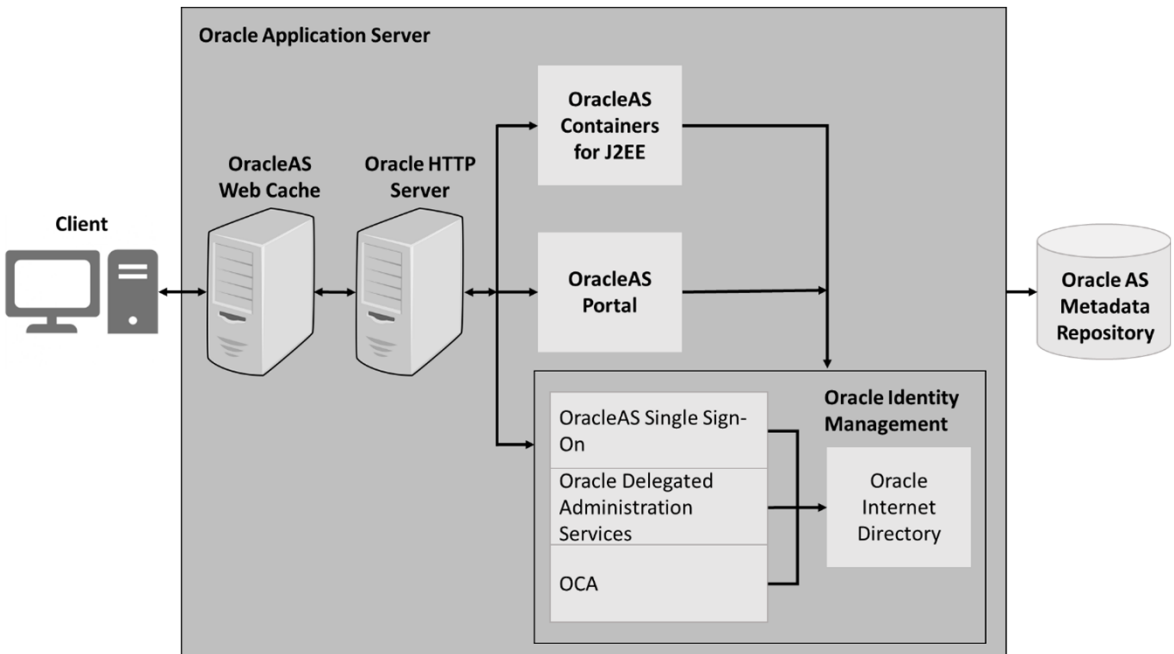
- Application Server Threats and Countermeasures
  - Network Eavesdropping
  - Unauthorized Access
  - Viruses, Worms, and Trojan Horses



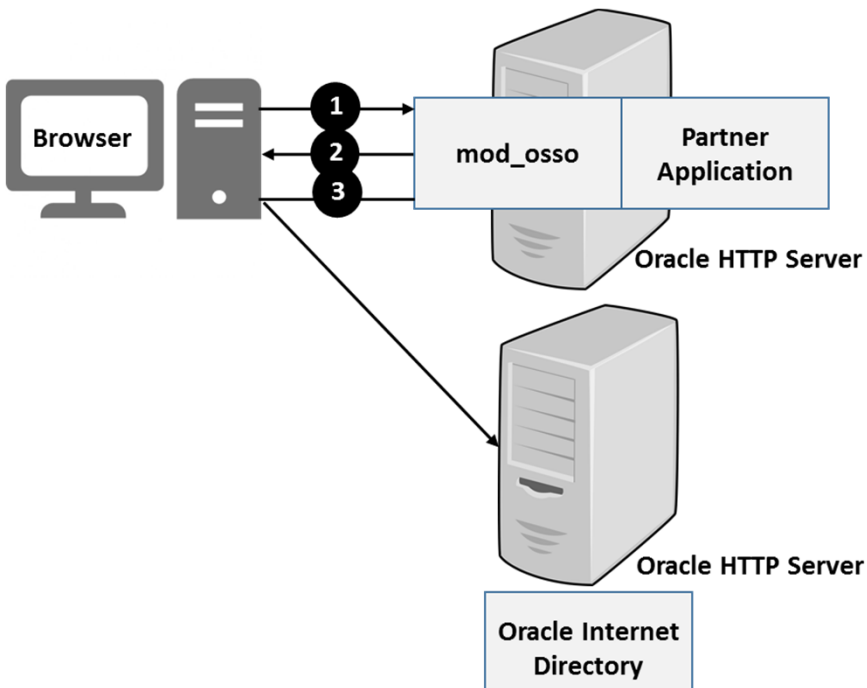
Introduction to Oracle Application Server

- Introduction to Oracle Application Server and security objectives
  - Providing Basic Security Services
  - Supporting Standards
  - Ensuring Deployment and Configuration Flexibility
  - Minimizing Application Development and Deployment Cost
  - Providing Security in Depth

Security architecture of oracle application server



Oracle HTTP Server Security



Single Sign-On With mod_osso

Oracle application server portal security

- Brief introduction about Oracle Application Server Portal Security

Oracle Application Server Security Best Practices (1 of 2)

- Explaining the oracle application server security best practices
  - Best practices for HTTPS Use
  - Best Practices for Cookie Security
  - Best Practices for Certificates Use

Oracle Application Server Security Best Practices (2 of 2)

- Explaining the oracle application server security best practices
  - Review Code and Content Against Already Known Attack
  - Follow Common Sense Firewall Practices
  - Leverage Declarative Security
  - Use Switched Connections in DMZ
  - Place Application Server in the DMZ
  - Secure Sockets Layer

Oracle Application Server Security Best Practices (2 of 2)

- Explaining the oracle application server security best practices
  - Review Code and Content Against Already Known Attack
  - Follow Common Sense Firewall Practices
  - Leverage Declarative Security
  - Use Switched Connections in DMZ
  - Place Application Server in the DMZ
  - Secure Sockets Layer

Web Application Server Security best practices

- Explaining the best practices of web application server security
  - Use separate servers for internal and external applications
  - Use Separate Development Server for Testing and Debugging Apps
  - Audit Website activity and store logs in a secure location
  - Education of developers on sound security coding practices
  - Patching Operating System and Web Server
  - Use of Application Scanners

Introduction of mobile application server security

- Understanding the mobile application server security

Introduction to OWASP (1 of 2)

- Introduction to OWASP and top 10 OWASP
  - Insecure Data Storage
  - Weak Server-Side Controls
  - Insufficient Transport Layer Protection
  - Client Side Injection
  - Poor Authorization and Authentication

Introduction to OWASP (2 of 2)

- Introduction to OWASP and top 10 OWASP
  - Improper Session Handling
  - Security Decisions via Untrusted Inputs
  - Side Channel Data Leakage
  - Broken Cryptography
  - Sensitive Information Disclosure

Mobile Application Security Testing

- We Can Divide Mobile Application Testing into Three Parts:
  - Dynamic analysis
  - Black box security testing
  - Static analysis & code review

Identifying and protecting

- Describing identifying and protecting data in mobile devices
  - Identify Sensitive Data?
  - Protecting Data - Things to Remember

Formidable App

- Describing the concept of formidable app
  - Creating a Formidable App
  - Steps to create a secure and powerful application

Security Testing Tools

- Explain the various security testing tools
  - Qasat
  - HashQ
  - Android Emulator
  - WebScarab
  - WebSlayer

Real-Time Examples

- Following are the real time examples:
  - Rogue Instagram Application
  - DroidDream

Checkpoint

1. Which component of the system security defines which sorts of Internet communications will be permitted into the corporate network, and which will be blocked?
   A. Web Browser
   B. Firewalls
   C. Load Balancers
   D. None of the above
2. Which of the following statements is/are NOT true about Secure Socket Layer?
   A. Provides secure communications over intranets and the Internet
   B. In SSL communication between two entities, such as companies or individuals, the server has a public key and an associated private key
   C. SSL uses both asymmetric and symmetric encryption to communicate
   D. All of the above statements are true
3. In which attack, the attacker places packet-sniffing tools on the network to capture traffic?
   A. Network eavesdropping
   B. Unauthorized access
   C. Trojan horses
   D. Worms

Checkpoint

4. Which of the following cannot be identified as security objectives for application server?
   A. Authentication
   B. Authorization
   C. Data Protection
   D. All of the above
5. When services available and software versions pertaining to an application server are given away due to banner grabbing, it corresponds to which threat?
   A. Banner threat
   B. Worm
   C. Unauthorized access
   D. None of the above
6. Choose the correct alternative from the following

Assertion (A): Load balancer ensures consistent application availability, even when one or more server fails

Reason (R): Load balancer distributes an application's load over many identically configured servers

   A. Both A and R are true and R is the correct explanation of A
   B. Both A and R are true but R is NOT the correct explanation of A
   C. A is false but R is true
   D. Both A and R are false

Checkpoint

7. Which of the following statements is NOT true for SSL keys?
   A. A symmetric encryption key (the bulk encryption key) is used to encode An asymmetric key (PKI public key)
   B. Asymmetric encryption has a performance cost due to its complexity
   C. The bulk encryption key is used to encrypt subsequent communication
   D. Both A and B
8. Choose the correct sequence of steps undertaken to negotiate an SSL session

   W) The client creates a bulk encryption key, often a 128 bit RC4 key, using a specified encryption suite.

   X) The server sends the client its public key.

   Y) The client encrypts the bulk key with the server's public key, and sends the encrypted bulk key to the server.

   Z) The server decrypts the bulk encryption key using the server's private key.

   A. WXYZ
   B. XWYZ
   C. ZXYW
   D. XYZW

Checkpoint

9. Which of the following is/are NOT application scanner tool(s)?
   A. Watchfire
   B. SUCURI
   C. AppScan24
   D. Both A and B
10. Which of the following is an attack associated with unauthorized access?
   A. Port scanning that detects listening services
   B. Banner grabbing that gives away available services and possibly software versions
   C. Malicious application input
   D. All of the above

Checkpoint solutions

1. B
2. D
3. A
4. D
5. C
6. A
7. A
8. B
9. C
10. D

Unit summary

Having completed this unit, you should be able to:

- Get acquainted with various application server threats and countermeasures
- Get an overview of general application server security overview
- Get familiar with the Oracle application server security architecture
- Understand the need of application server security

Database Server Security

Unit objectives

After completing this unit, you should be able to:

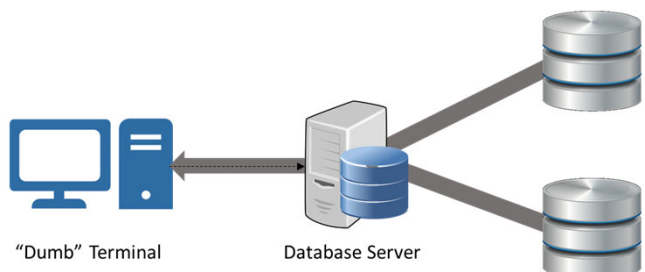
- Get an overview of the need of database server security mechanisms
- Get familiar with the methodology of securing open source databases
- Understand the role of database administrator in securing database server
- Know the components of database security assessment

Introduction to Database Server Security

- A brief introduction of database server security and its importance
  - Introduction
  - Importance of Database Server Security

Architecture for Database Systems

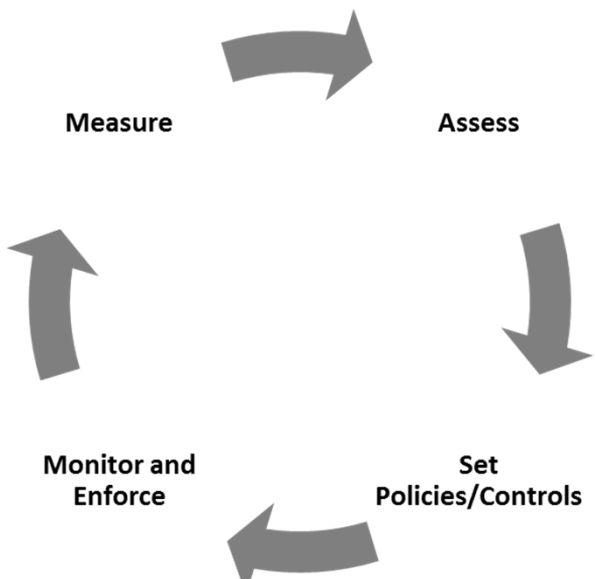
- Explaining the Architecture for Database Systems and it provide:
  - Independence of data and programs
  - Ease of system design
  - Ease of programming
  - Powerful query facilities
  - Protection of data



Direct connection with database server

Database attacks,security & lifecycle

- Defining the different database attacks and security
  - Insider Threat
  - Login Attacks



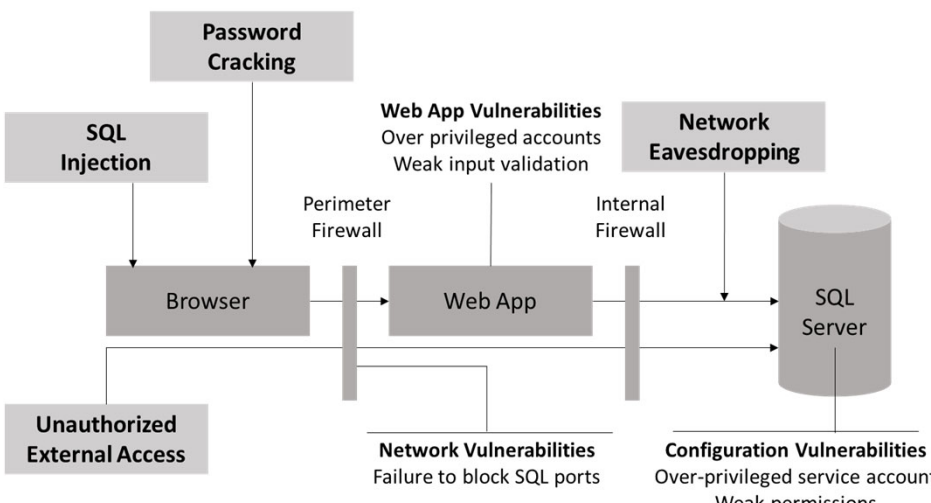
Need of Database Server Security

- Following are the database vulnerabilities
  - Lack of security feature maturity Login Attacks
  - Database Password Management
  - Oracle Internal Password
  - Oracle Listener Process password
  - Oracle Internal Password - “orapw” File Permission Control
  - Operating system back doors
  - Auditing
  - Trojan Horses

	MS SQL Server	Sybase	Oracle 7	Oracle 8
Account Lockout Facility	No	No	No	Yes
Rename Admin Account	No	No	No	No
Require Strong Passwords	No	No	No	Yes
Stale Accounts	No	No	No	No
Password Expiration	No	Yes	No	Yes
Login Hours Restriction	No	No	No	No

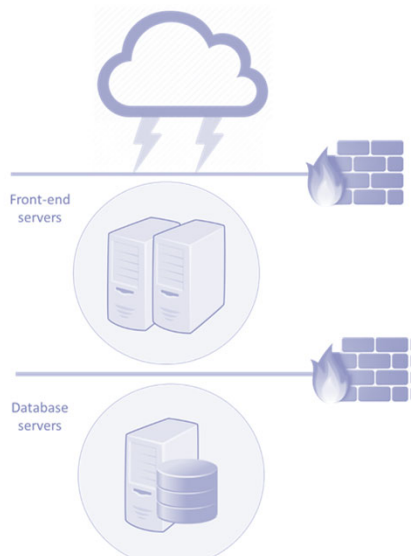
Database Server threats & countermeasures

- Following are the database vulnerabilities
  - SQL Injection
  - Network Eavesdropping
  - Unauthorized Server Access
  - Password Cracking



Acquiring Database and Server Security

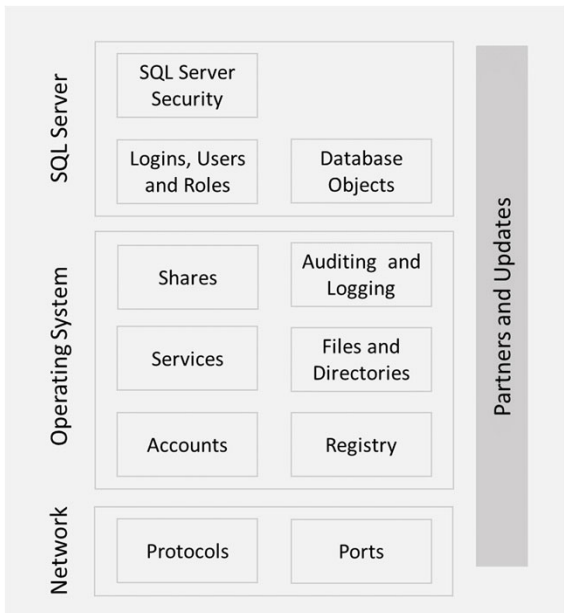
- Explaining the database acquiring and server security mechanisms
  - NAT and PAT
  - A demilitarised zone (DMZ)
  - Content-based firewalls
  - SSL connections
  - IPSec security



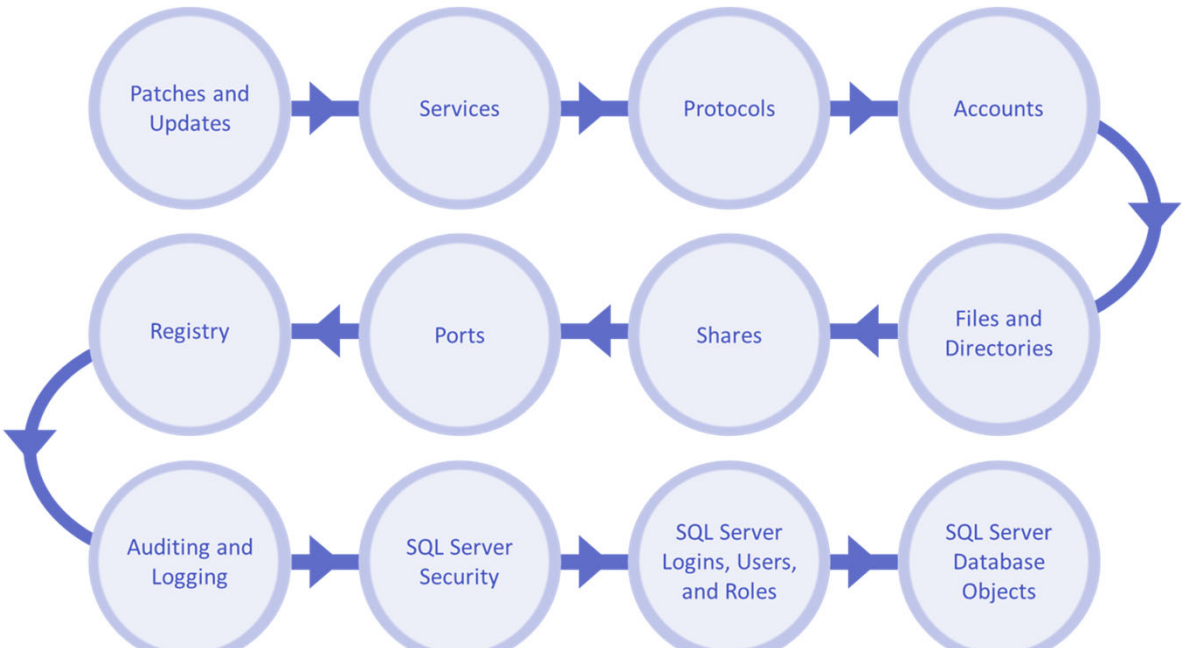
Database server farm

Securing Open Source Databases

- How to secure open source database and its methodology
  - Patches and Updates
  - Services
  - Protocols
  - Accounts
  - Files and Directories
  - Shares
  - Ports
  - Registry
  - Auditing and Logging
  - SQL Server Security
  - SQL Server Logins, Users, and Roles
  - SQL Server Database Objects



Steps for Securing Database Server



Best Practices to secure database server

- Database server secure practices and planning
  - Strong Password Policy Execution
  - Discard all Default Users and Demo-test Databases
  - Change the Admin User Name
  - User Privileges Need to be Restricted
  - Disable Public Network Access to Database Servers
  - Enforce SSL/TLS on Remote Connections and Restrict IP
  - Check for Database Dumps in Public Locations
  - Encrypt Your Application Files and Backups
  - Web Application Firewall and Malware Scanner Should be used
  - Always keep the Software Updated

Security checklist (1 of 2)

- Security checklist for a Database Administrator with various operations
  - Installation & Configuration
  - Operations & Maintenance

Security checklist (2 of 2)

- Security checklist for a Database Administrator in various tasks
  - Backup & Recovery
  - Web-based Databases

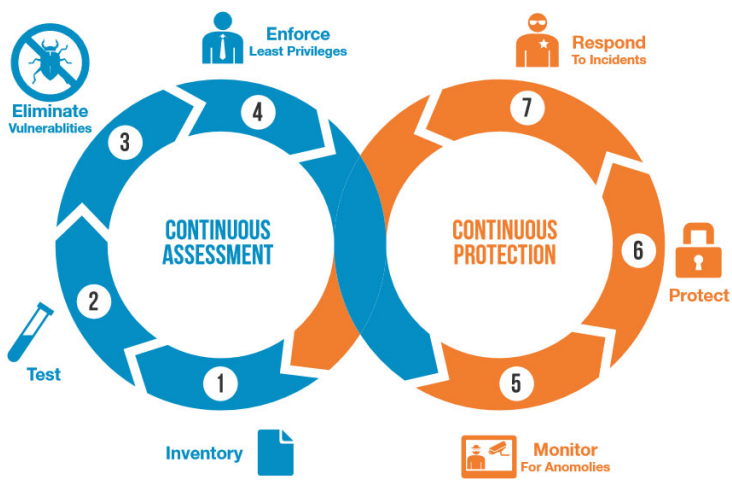
Invalid Data	**This is the smallest, but most common database problem. It occurs when a finite number of invalid entries find their way into the data.**
Corrupted Database Object	The next level of database problems includes situations in which a single or limited number of database objects have become corrupted or invalid.
Full Database Corruption	At this level, the scope of the problem is so significant that the database is no longer operational and a full database recovery must be performed.
Multiple Database Corruption	The largest levels of database problems occur when multiple databases within the organization have been corrupted and must be recovered as a set.

Database Security Assessment

- Following four attributes of a best practice database security assessment
  - Impact on production systems
  - Accuracy
  - Efficiency
  - Breadth of analysis
- Barriers of database security assessment

Database Security Program Design (1 of 2)

- Explaining the DB security programme design and its process with checklist
  - Define a database security program with actionable processes
  - Clarify the scope of your program through database discovery and inventory
  - Define security standards and compliance policies
  - Conduct vulnerability and configuration assessments



Database Security Program Design (2 of 2)

- Explaining the DB security programme design and its process with checklist
  - Define a database security program with actionable processes
  - Clarify the scope of your program through database discovery and inventory
  - Define security standards and compliance policies
  - Conduct vulnerability and configuration assessments

Authorized users	Privileged users	Knowledge users	Outsiders with insider access and/or vulnerability knowledge
Employees such as clerks, accountants, finance staff, sales people, purchasing staff and others. This type of user includes anyone granted authorized access to the data or systems within a given enterprise.	Individuals with elevated privileges, broad access and extensive database knowledge, such as: DBAs, developers, quality assurance staff, contractors and consultants.	Users with access and knowledge of systems or security protocols like IT operations, network operations, security and audit personnel.	These users may not have the same user rights as “Authorized”, “Privileged”, or “Knowledge” users do, but they may be capable of performing privileged activity.

Checkpoint

1. Which of the following is NOT a feature of a good database system architecture?
   A. Independence of data and programs
   B. Ease of system design
   C. Powerful query facilities
   D. Dependency on data and programs
2. Which of the following statement(s) is/are NOT true for Client/server architecture of database systems?
   A. The database server and the database and other resources are placed at one location while the code for application is placed on a client machine or on their personal computer
   B. The database server and the database and other resources and the code for application are placed at the same location to ease the operation and access to database
   C. Queries are carried to the server machine and the resultant data is carried back to the client's machine by pre-defined queries
   D. Queries are processed on the database server, while rest part is done on the workstation
3. In slim client architecture, higher security requirements are required on the
   A. Client side
   B. Application server
   C. Back-end server databases
   D. None of the above

Checkpoint

4. In slim client architecture, changing number of security requirements are required at the
   A. Application server
   B. Client side
   C. Back-end server databases
   D. None of the above
5. Which type of threats on database can lead to denial of service attack (DOS)?
   A. Logical threats
   B. Physical threats
   C. Databases are inherently immune to DOS attacks
   D. Both A and B
6. Which of the following is NOT a countermeasure against SQL injection in a database server?
   A. Sanitization of input data by application before using it in SQL queries
   B. Usage of SQL server login that executes permissions only to selected stored procedures
   C. An application should constrain input data before using it in SQL queries
   D. All of the above are a countermeasure against SQL injection

Checkpoint

7. Which of the following is a vulnerability associated with Unauthorized database server access?
   A. Lack of IPSec or TCP/IP filtering policies
   B. Failure to block the SQL Server port at the perimeter firewall
   C. Both A and B
   D. Neither A nor B
8. Which of the following database security mechanisms are equipped with the capability to look into the data packets owing in either direction, and provide systems administrators a means to configure actions based on the intercepted content?
   A. Content-based firewalls
   B. SSL connections
   C. A demilitarised zone (DMZ)
   D. None of the above
9. Which of the following database security mechanisms uses public-key and private-key cryptography to encrypt all connections between caller and listener?
   A. IPSec security
   B. Content-based firewalls
   C. SSL connections
   D. A demilitarised zone (DMZ)

Checkpoint

10. Which of the following is one of the best practices to secure database server?
    A. Discard all default users and demo-test databases
    B. Change the admin user name
    C. Restrict user privileges
    D. All of the above

Checkpoint solutions

1. D
2. B
3. B
4. C
5. A
6. D
7. C
8. A
9. A
10. D

Unit summary

Having completed this unit, you should be able to:

- Get an overview of the need of database server security mechanisms
- Get familiar with the methodology of securing open source databases
- Understand the role of database administrator in securing database server
- Know the components of database security assessment

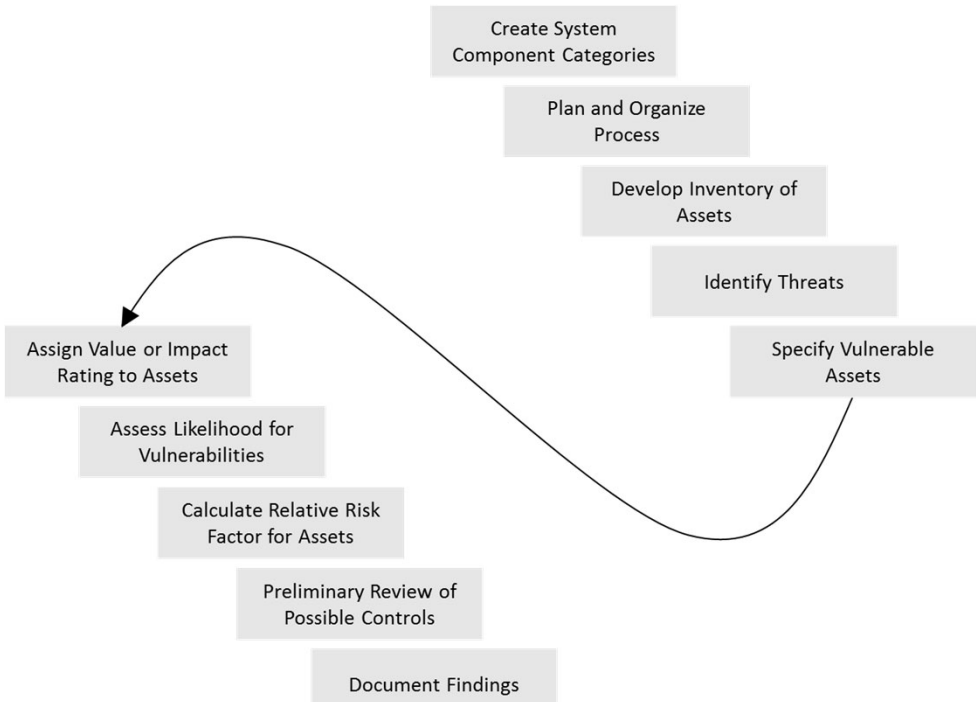
IT System Security Processes

Unit objectives

After completing this unit, you should be able to:

- Know how to identify assets, threats and vulnerabilities before applying system security mechanisms
- Understand importance of examining tools, techniques and technologies involves in system security processes
- Understand when and where to apply operational controls
- Get an insight on the aspects involved in implementation of security policy

Identification of risk



Risk Identification Process

Organizational Assets Used in Systems

IT System Components	Risk Management Components	
People	People inside an organization	Trusted employees Other staff
Procedures	Procedures	IT business and standard procedures IT business and sensitive procedures
Data	Data/Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking components	Intranet components Internet or Extranet components

Identifying assets

- Here we can identifying various assets
  - Identifying Hardware, Software, and Network Assets
  - Identifying People, Procedures, and Data Assets
  - Classifying and Categorizing Assets

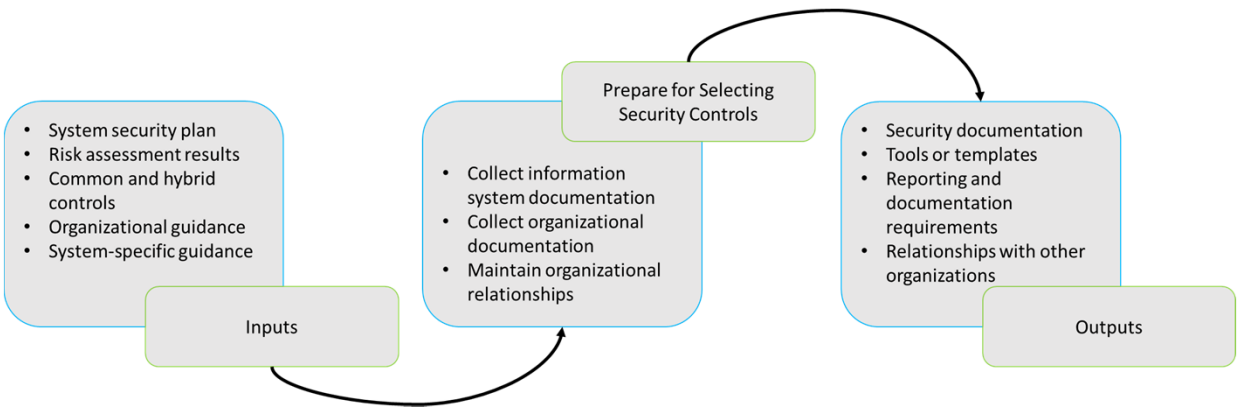
Threat Identification

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of system or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightening
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Prioritizing System Vulnerabilities

	High Likelihood	Medium Likelihood	Low Likelihood
High Impact	Sensitive information stored on an unencrypted laptop	Tape backups taken offsite that are not encrypted and/or password protected	No administrator password on an internal SQL Server system
Medium Impact	Unencrypted e-mails containing sensitive information being sent	Missing Windows patch on an internal server that can be exploited using Metasploit	No passwords required on several Windows administrator accounts
Low Impact	Outdated virus signatures on a standalone PC dedicated to Internet browsing	Employees or visitors gaining unauthorized network access	Weak encryption ciphers being used on a marketing website

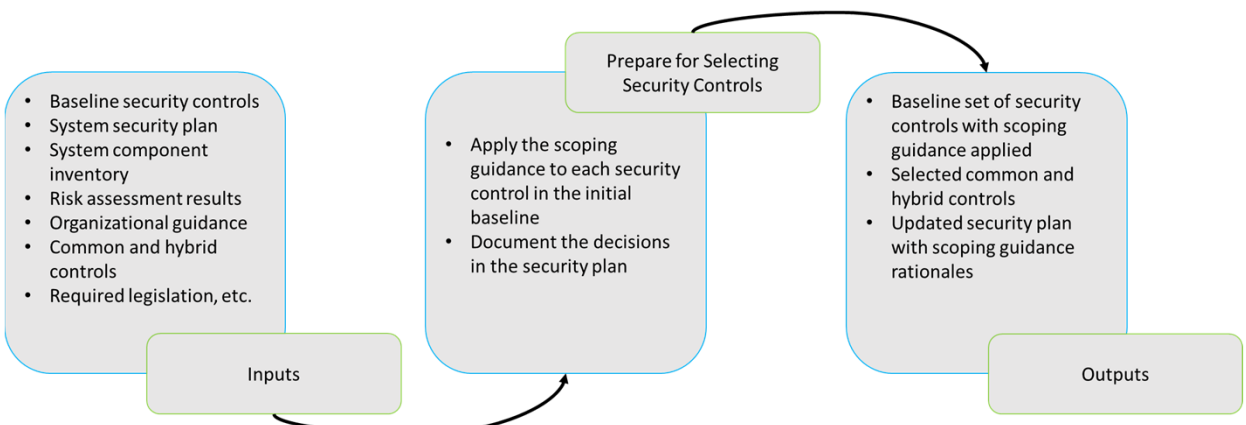
Prepare for Selecting Security Controls



Initial Security Control Baseline

No.	Control Name	Tailoring	Rationale
AC-1	Access Control Policy and Procedure		
….			
AC-3	Account Enforcement		
….			
AT-3	Security Training		
AT-4	Security Training Records		
….			
CP-2	Contingency Plan		
CP-3	Contingency Training		
….			
IA-3	Device Identification and Authentication		
IA-4	Identifier Management		
….			
PE-14	Temperature and Humidity Controls		
PE-15	Water Damage Protection		
….			
SC-12	Cryptographic Key Establishment and Management		
….			
SI-11	Error Handling		
SI-12	Information Output Handling and Retention		

Apply Scoping Guidance (1 of 2)



Apply Scoping Guidance (2 of 2)

- The application of appropriate scoping guidance to the initial baseline
  - Apply Security Objective-related Considerations
  - Apply Common Control-related Considerations
  - System Component Allocation-related Considerations
  - Apply Scalability-related Considerations
  - Document the Decisions in the Security Plan

Analyzing System Environment

- A brief description of the technical system is provided which includes any environmental or technical factors that raise special security concerns, such as:
  - The system is connected to the Internet;
  - It is located in a harsh or overseas environment;
  - Software is rapidly implemented;
  - The software resides on an open network used by the general public or with overseas access;
  - The application is processed at a facility outside of the organization's control; or
  - The general support mainframe has dial-up lines.

Planning for security in the system lifecycle

- Few basic phases of IT system lifecycle
  - Initiation Phase
  - Development/Acquisition Phase
  - Implementation Phase
  - Operation/Maintenance Phase

Applying Operational Controls (1 of 2)

- Describing the operational control measures
  - Personnel Security

Applying Operational Controls (2 of 2)

- Describing the operational control measures
  - Physical and Environmental Protection

Contingency Planning

- Briefly describing the contingency plan

Maintenance controls

- Maintenance controls with examples

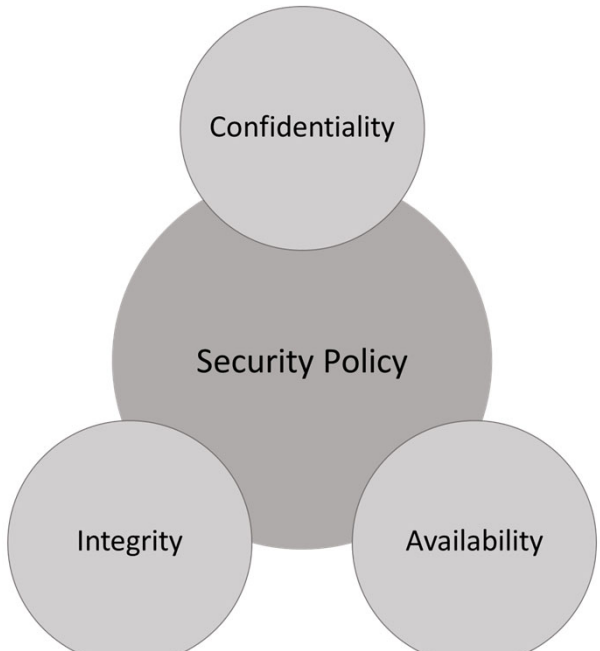
Data integrity/validation controls

- Describing the Data integrity/validation controls
  - Various data integrity/validation Controls
  - Malicious Programs
  - Virus Protection
  - Message Authentication
  - Integrity Verification
  - Reconciliation

Documentation

- Examples of documentation for major application

Implementing Security Policy



Scope of security policy properties

Security considerations

- Explaining the security considerations in system support and operations

Important security considerations (1 of 2)

- Important security considerations within some of the major categories
  - user support,
  - software support,
  - configuration management,
  - backups,

Important security considerations (1 of 2)

- Important security considerations within some of the major categories
  - media controls,
  - documentation
  - maintenance

Checkpoint

1. Which one of the following is an attribute to be considered when deciding which attributes to track for each information asset?
   A. MAC address
   B. Serial number
   C. Manufacturer name
   D. All of the above
2. What is the step prior to determining whether asset categories are meaningful to the organization's risk management program?
   A. Threat identification
   B. Classification and categorization of assets
   C. Identification of data assets
   D. None of the above
3. When public access-related considerations are being applied, what is the correct step to be taken in the case the security control does not apply to the system?
   A. Mark the control in the spreadsheet/table as does not apply
   B. Explain the rationale justifying why the control does not apply
   C. Identify the specific components related to the control in the spreadsheet/table
   D. Both A and B

Checkpoint

4. In which phase of the IT system life cycle, system is designed, purchased, programmed, developed, or otherwise constructed?
   A. Initiation phase
   B. Development/acquisition phase
   C. Operation/maintenance phase
   D. Implementation phase
5. Who ensures that custodial and building maintenance personnel entering the computer room are under continuous visual observation at all times by a person with authorized unescorted access?
   A. Head of IT department
   B. The data center manager
   C. The system manager
   D. Both B and C
6. Which controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected?
   A. Data integrity/validation controls
   B. Maintenance controls
   C. Software controls
   D. None of the above

Checkpoint

7. Security policy can be enforced by
   A. individuals
   B. by devices in the physical environment
   C. by automated mechanisms implemented in the hardware, firmware, and software of the system
   D. All of the above
8. Which property of the security policy deals with protections against unauthorized access and unauthorized disclosure of resources?
   A. Availability
   B. Integrity
   C. Confidentiality
   D. Technicality
9. Which of the following is not true for software support while implementing security policy?
   A. It should be ensured that software has not been modified without proper authorization
   B. It should be easily recognizable which problems (brought to their attention by users) are security-related
   C. Care is given to the configuration and use of powerful system utilities
   D. Both A and C

Checkpoint

10. Which controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and another media?
    A. Media controls
    B. Software controls
    C. Hardware controls
    D. None of the above

Checkpoint solutions

1. D
2. D
3. D
4. B
5. D
6. B
7. D
8. C
9. D
10. A

Unit summary

Having completed this unit, you should be able to:

- Know how to identify assets, threats and vulnerabilities before applying system security mechanisms
- Understand importance of examining tools, techniques and technologies involves in system security processes
- Understand when and where to apply operational controls
- Get an insight on the aspects involved in implementation of security policy