**BTM 618 Network Technologies**

**Class Schedule:** Monday 5:00-8:30 pm August 29 – October 23

**Class Location:** SBL 207

**Instructor: Cary Barker**

|  |  |
| --- | --- |
| Cary BarkerAdjunct Faculty Information SystemsStevenson University10945 Boulevard Circle Owings Mills, Maryland 21117-7804 | Email: cbarker at Stevenson.eduweb site: http://carybarker.comBlackboard: [http://blackboard.Stevenson.edu](http://iclass.Stevenson.edu)  |

**Course Text:**

|  |
| --- |
| Hassell, Jonathan (2008)Windows Server 2008: The Definitive GuideISBN: 978-0-59-651411-2Safari Online: <http://search.safaribooksonline.com/9780596514112>  |

**Course Description:**

This course demonstrates methods of protecting the Windows environment from inside threats as well as external vectors. This course develops skills and knowledge necessary to secure a Windows Server and provides the knowledge and experience to securely install, configure, patch, harden, implement secure group policy, scan for weaknesses, audit and remediate security compromises in a Windows Enterprise server environment.

**Course Materials**:

Windows Server 2008: The Definitive Guide

USB memory stick or USB hard drive

Online Resources:

Windows 7SP1 RSAT http://www.microsoft.com/download/en/details.aspx?id=7887

Microsoft MBSA 2.2 <http://technet.microsoft.com/en-us/security/cc184923.aspx>

Microsoft WSUS 3.0 SP2 http://technet.microsoft.com/en-us/wsus/bb332157

# Course Goals:

* Define the procedures necessary for securely deploying new systems and the risks for failing to follow proper procedure
* Explore the process of securing the entire domain using Active Directory group policy
* Explain standardization, change management, the ‘gold standard’ and best practices in relation to Windows Enterprise security
* To provide the student practical experience in securely installing, configuring, auditing, probing the security of, and remediating Windows systems.
* To review an array of tools that can be used in support of Windows security and/or to compromise that security.

# Learning Outcomes:

* At the end of this course, students will:

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[x]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[x]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[x]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

# Learning Strategies:

Learning outcomes will be achieved through the following strategies:

* Guided Independent online research and readings
* Class discussion
* Class Labs
* Online quizzes
* Final Lab

**TABLE OF CONTENTS**

[Course Goals: 2](#_Toc207595450)

[Learning Outcomes: 2](#_Toc207595451)

[Learning Strategies: 2](#_Toc207595452)

[Grading Table 1](#_Toc207595453)

[Late Work/Assignment Makeup, Citations, Attendance, and Email Policy 2](#_Toc207595454)

[Email Policy: 2](#_Toc207595455)

[Quiz Policy: 2](#_Toc207595456)

[INFORMATION SYSTEMS DIVISION STUDENT & FACULTY COMMUNICATION GUIDELINES 3](#_Toc207595457)

[Course Schedule 4](#_Toc207595458)

[Course Assignments 5](#_Toc207595459)

[AIT 618 DELIVERABLES 5](#_Toc207595460)

[Course Readings 6](#_Toc207595461)

[Professionalism Assessment Grading 8](#_Toc207595462)

[LAB1: Windows Core 9](#_Toc207595463)

[LAB 1:Windows Core Evaluation Criteria 10](#_Toc207595464)

[LAB2: Group Policy 11](#_Toc207595465)

[LAB 2 Evaluation Criteria 12](#_Toc207595466)

[LAB3: Implement WSUS and MBSA 16](#_Toc207595467)

[LAB 3 Evaluation Criteria 17](#_Toc207595468)

[LAB4: Implement Centralized Windows Audit system 20](#_Toc207595469)

[LAB 4 Evaluation Criteria 21](#_Toc207595470)

[Final Exam 24](#_Toc207595471)

[Stevenson University Policies 25](#_Toc207595472)

[REFERENCE MATERIALS AND RESOURCES 27](#_Toc207595473)

[Online Research Resources 28](#_Toc207595474)

[Course Bibliography 29](#_Toc207595475)

# Grading Table

|  |  |
| --- | --- |
| **Assignment** | **points** |
| Professionalism | 5 |
| Class participation | 25 |
| Labs | 40 |
| Final Lab | 30 |
| TOTAL | 100 |

**Note: Improper, distracting, disrespectful or disruptive behavior in the classroom or anything less than professional and respectful email communication will result a severe grading penalty beyond the breakdown noted above at the discretion of the instructor. Any violation of the Academic Honesty Policy or the policies detailed in this syllabus may result in an ‘F’ for the assignment or an ‘F’ for the course at the discretion of the instructor. The penalty for a violation of the Academic Honesty Policy could be changed to dismissal from the college by higher authorities.**

**Grading Policy:**

In compliance with the Stevenson University, Graduate School grading policy, a student’s performance in a course will be measured in accordance with the following grading system:

|  |  |  |
| --- | --- | --- |
| A = 4.0 | Excellent: | ***Outstanding achievement and initiative exceeding course requirements.*** |
| B = 3.0 | Good: | Work meeting minimum course requirements at the graduate level. |
| C = 2.0 | Unsatisfactory: | Work failing to meet the minimum course requirements. It is the lowest possible passing grade. |
| F = 0.0 | Failure: | Academic Probation |
|  |  |   |

The grade of 'C' is the lowest acceptable grade and only one can be awarded during the program.

The grade of 'B' represents work meeting minimum course requirements at the graduate level. The student receiving a grade of 'B' has consistently demonstrated a complete understanding of the material and concepts presented throughout the course. Additionally, the student has completed all course requirements on time, exhibited enthusiastic interest in topics and discussions and is able to present and apply course concepts in a clear and organized manner, both verbally and on written tests.

The grade of 'A' is awarded only to those students who fully meet this standard, who additionally demonstrate exceptional comprehension and application of the course material, and demonstrate initiative in exceeding course requirements.

Late Work/Assignment Makeup, Citations, Attendance, and Email Policy

## Late work and make up exam policy:

Students will not receive credit for assignments submitted late or missed exams without **prior** approval of the instructor. Only in the most extreme circumstances may students petition the instructor for exemption. The instructor will consider all petitions, deny those deemed other than extreme, and grant those were evidence is clear. At the discretion of the instructor, the student may be required to petition the Division Director Information Systems for exemption. The process requires an in person interview with the Division Director Information Systems and a detailed formal letter of explanation which shall cite, among other items, the personal contact information for verification of required references. Further details of the process and the documentation required can be obtained from the instructor.

## Citations - APA Guidelines

All written work for courses in the Information Systems program must cite sources using the APA citation style, applied as endnotes at the end of your research paper. Footnotes or inline citations are not permitted. Note that in APA style citations the date of publication is closer to the beginning. Since authors of technology articles tend to publish articles frequently as technology changes, using the APA citation style makes it easier to differentiate sources.

## Attendance Policy:

Students are responsible for all information covered in class and the timely delivery of out of class assignments regardless of attendance. If a class is missed for any reason it is the student’s responsibility to obtain from a classmate all information covered in class including but not limited to instructors lecture, class instructions, class notes, assignments, or any other relevant materials. All information provided in Information Systems courses is to be considered “essential content”. Failure to attend class does not exempt the student from assignment deadlines nor does it exempt the student from the responsibility of understanding testable concepts as well as concepts and skills required as a prerequisite to other courses in the curriculum. In all cases students must notify faculty in advance of any missed class session.

# Email Policy:

All college email communication will be exchanged **only over Stevenson University email accounts**. Students are responsible for the information sent to their Stevenson University email account and must monitor their Stevenson University accounts each day for important college and course related information. Students are required to view their Stevenson University email accounts directly or set up their Stevenson University email account to forward to an account they view regularly during the day. If you are not receiving regular information over a forwarded email address you should immediately investigate the problem before missing important instructions or announcements. Students should also note that email messages in their MAILBOX and personal mail folders are routinely purged on a regular schedule.

# Quiz Policy:

* All quizzes must be completed online before the start of class
* Quizzes are open book and open note
* Quizzes are to be completed by the student without any assistance from other students or any other party. Students found to have had outside help will receive a “0” for that quiz and will be notified outside of class.

INFORMATION SYSTEMS DIVISION
STUDENT & FACULTY COMMUNICATION GUIDELINES

Effective communication between students and faculty is essential for student success and faculty expectations. The process below is designed to help everyone feel comfortable that their message is successfully delivered and acknowledged. Students and faculty should use the steps below to close the loop in contacting each other. Note that for questions requiring a more immediate response, students should contact faculty by telephone on their office extension.

1. Student emails faculty with question or deliverable.
2. Within one business day or as soon as the faculty sees the message, the faculty sends an email message in response that acknowledges receipt and review of message from the student. (not necessarily an answer)
3. If the student does not get a response acknowledging the receipt within one business day, the student should send the message again. If no acknowledgement is received, the student should call the faculty member on their office extension or the phone number listed in the course syllabus.
4. If the student is still unable to reach the faculty member, they should then contact Ken Snyder by email on ksnyder@mail.Stevenson University.edu
5. Within 96 hours or sooner if project deadlines are involved, the faculty will respond with a feedback message on questions or assignments.
6. Students will respond with an acknowledgment of the feedback message from the faculty.

## Student Responsibilities:

Students are responsible for communication with their instructor. There should be no delay in asking questions, expressing concern about the clarity of concepts or requesting feedback on assignments.

IMPORTANT:

* In all email communications with the instructor, students must identify themselves in the subject line of the message to include: **Last Name, First Name, Course Number, and Section Number.**
* All college email communication will be exchanged **only over Stevenson University email accounts**. Students are responsible for the information sent to their Stevenson University email account and must monitor their Stevenson University accounts each day for important college and course related information. Students are required to view their Stevenson University email accounts directly or set up their Stevenson University email account to forward to an account they view regularly during the day.

Students should expect to receive a great deal of information over their Stevenson University email account. If you are not receiving regular information over a forwarded email address you should immediately investigate the problem before missing important instructions or announcements.

# Course Schedule

‘Guide’ means the Windows Server 2008: The definitive Guide

**CHECK BLACKBOARD FOR ANY MODIFICATIONS TO ASSIGNMENTS, DUE DATES, ETC.**

**The below should be taken as a guideline for the class, it is not written in stone**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Week** | **Date** | **Pre-Class Assignment** | **Topic** | **In Class Activity** |
| Pre-Class | Aug 22 | Read Chapters 1-2 Guide | Introduction to the ClassComputer Security basicsInstalling WindowsSecure Network Architecture | NA (Blackboard) and home |
| Week 1 | Aug 29 | Read Chapters 1-2,9 Guide | VMWARE Lab Manager tourWindows Security basicsInstalling WindowsWindows Physical SecurityWindows Core | Class Discussion Introductory Lab. |
|  | Sept 5 |  | College closed Labor Day |  |
| Week 2 | Sept 12 | Read Chapter 3,4, 5 Guide | File system SecurityDNS securityIPv4,IPv6 and network commandsActive Directory | Class Discussion Windows Core/Active Directory Lab 1 |
| Week 3 | Sept 19 | Read Chapter 6 Guide | Active Directory, AD security, Users and Group Policy | Class Discussion Lab 2: Group Policy |
| Week 4 | Sept 26 | Lab: Group Policy dueRead Chapter 7 Guide *Windows Server 2008 Security Guide*\*\* | System hardening, monitoring, auditing, patching and updating. | Class Discussion Lab 3: system security  |
| Week 5 | Sept 3 | Read Chapter 11 GuideRead the following:[**Introduction to Network Access Protection**](http://www.microsoft.com/technet/network/nap/napoverview.mspx)**\*\*\*** | Remote Access securityCertificate ServicesNetwork Access Protection – DHCP/802.1x/IPSEC, etc. | Lab 3 dueClass Discussion Lab 4: Network Access Protection |
| Week 6 | Oct 10 |  | Network Access Protection – DHCP/802.1x/IPSEC, cont. | Class Discussion Lab 4: Network Access Protection cont. |
| Week 7 | Oct ?? | Lab 4 due | Final Lab | All labs due Oct 14 at 5PM |
|  |  |  |  |  |

\* <http://www.microsoft.com/windows/products/winfamily/virtualpc/support.mspx> - select the Virtual PC tour. Specifically watch the “Virtual PC in Action” part of the tour

\*\* Windows 2008 Security Guide <http://technet.microsoft.com/en-us/library/cc264463.aspx>

\*\* \* links available from the main NAP Microsoft page at <http://technet.microsoft.com/en-us/network/bb545879.aspx>

Course Assignments

The following deliverables are required. The schedule for delivery and detailed requirements can be found on the pages to follow.

* Course Readings
* Class discussion
* Professionalism
* Labs
* Final Lab

# AIT 618 DELIVERABLES

|  |  |
| --- | --- |
| **DELIVERABLE**  | **DUE**  |
| Readings | Weekly |
| Class discussion | Weekly |
| Labs | Weekly |
| Final Lab | Last Class |

# Course Readings

## Outcomes:

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[x]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[x]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[x]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

## Description/Requirements:

It is expected that students complete readings for each prior to class. For example, readings for session 2 should be read before attending the second class session. Please see the course schedule for additional detail on the readings due before each class session.

## Grading/Points Possible:

This assignment will not be assessed formerly. However content from readings will be assessed indirectly through all course assignments.

# Class participation

## Outcomes:

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[x]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[x]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[x]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

*Description/Requirements:*

Students will be graded on their contribution to in-class and asynchronous, online discussions. Students shall be graded on answering questions and contributing to the discussion on the subject of a class on any given night. Contribution is an essential learning process and shows that one can do more than regurgitate what has been read in a book. Students will be graded as follows:

1. Participating in online discussions regarding a specific weekly topic (minimum two posts per week).
2. Asking questions pertinent to the subject of the class.
3. Answering questions asked by the professor and/or other students.
4. Otherwise contributing to the class my making suggestions, helping others etc

Obviously students must be present that week to contribute to the class. If for some reason a student misses the whole or a significant part of the class for the week, they may make up the grade by finding and pointing out an incorrect fact presented by the professor. They must have references or be able to demonstrate what the fast should be. This is not a simple task; it is suggested you don’t miss class.

# Professionalism

## Outcomes:

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[x]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[x]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[x]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

*Description/Requirements:*

Professionalism is a graded assessment in all Information Systems courses. The Professionalism assignment is based on two key themes found in all Information Systems courses:

1. “The classroom is the workplace.”
2. “Students are professionals in the workplace.”

As in the workplace, students in information systems courses receive performance appraisals. These weekly performance appraisals are a measure of the students “Professionalism”. Professionalism is evaluated based on these criteria:

1. Respectful
2. Responsible
3. Readiness to Learn
4. Timeliness

The “Professionalism Assessment Grading” table that follows provides a model for those behaviors employers seek out and those they disdain in prospective employees. Employers contributed many of these behavior examples. While employers are certainly interested in a prospective employee’s technical knowledge, employers are only interested in hiring those with a professional attitude. A professional attitude is essential for success in the workplace and it is essential for success in the IT classroom. This should be an easy component of the grade to attain for everyone. Just review those positive behaviors in the chart, emulate them in the classroom and emulate them in all communication with fellow students and the faculty member.

Contributing to class discussions is a vital component of the course and the professionalism grade. It’s a measure of the student’s interest and level of familiarity with the information being discussed. Most importantly, participation in the group discussions elevates the group’s knowledge as a whole and makes the course more meaningful to all. Each student is expected to contribute by way of offering supporting information or posing questions about the topic during the evening’s discussions. Each student should join in the group discussions at least once per class. No one should feel that they have nothing to contribute. Everyone’s opinion and need for clarification is valid. Please share your thoughts, comments, and questions with us.

*Grading/Points Possible:*

This assignment is worth 5 points. This grade will be assessed weekly according to the behaviors detailed in the Professionalism Assessment Grading table that follows.

# Professionalism Assessment Grading

|  |
| --- |
| **Students will be evaluated based on in class and email communications using the professionalism criteria below. Review the behaviors below carefully. Your score for each section will be calculated by multiplying the potential points by the percentage rounded up to the nearest integer. It is the student’s responsibility to explicitly and consistently demonstrate these attributes to the faculty member who will be making a subjective value judgment regarding the student’s professionalism.** |
| **Behavior** | **Potential Points** | **0%** | **25%** | **75%** | **100%** | **Total** |
| **Responsible****(Contributor)** | **1.25** | The participant consistently failed or refused to participate in discussions. Participant is unreliable, shows no initiative.ORParticipant is not prepared for class discussions. | Participant shows some responsibility and initiative, respects the standards though may not always adhere to them.Seldom participates in discussion. | Occasionally, contributes ideas and thoughts on discussion topicsComes to class prepared and occasionally makes an effort to contribute. | Participant always comes to class prepared and is ready to discuss topics armed with ideas and questions.Participant assesses concepts being discussed, contributes ideas, views, and comments frequently. |  |
| **Respectful** | **1.5** | Participant was rude or abusive to other course participants or the instructor. ORParticipant persists in talking or creating a distraction while the instructor or another student is speaking. | Confrontational attitude towards instructor or other students while participating in discussions or posing questions. | Participant is passive and is not engaged in the class activities. | Participant is always polite and respectful. Does not interrupt others or talk privately while someone is speaking. |  |
| **Ready to Learn****(Listener)** | **1.25** | Participant tends to play a passive or disruptive role in the class, persists in talking while the instructor or another student is speakingORParticipant is not seated and logged on to the Stevenson University network or other required software prior to the start of the class session. | Participant is preoccupied and not focused on the speaker and is occasionally a distraction. | Participant listens. | Participate is an attentive listener, visibly engaged, and comprehends the subject.Participant seated and logged on to the Stevenson University network or other required software prior to the start of the class session. |  |
| **Timely** | **1** | Missed a class with out providing the instructor advanced notice and a valid excuse.Fails to turn in assignments or obtain notes from other students. | Periodically shows up late to class which creates a distraction for other students.OR Fails to meet deadlines. | Participant is punctual, gets work done one time,  | Participant is always on time for class and consistently meets assignment deadlines. |  |
|  |  |  |  |  | **Total points:** |  |

Participant’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Extra Credit

Extra credit is available for the course. Students may request an extra credit project, or they can find a factual error with the course as delivered by the professor. Finding a factual error in the class book (or syllabus) does not count!

In order to get credit for the factual error, the student must identify the fact the instructor gave in error and find out what the correct information is – with references that prove the fact beyond a reasonable doubt. Credit will be given based on the importance of the fact; generally from ½ to 2 points. Remember, this doesn’t sound like much until one realizes the entire class is worth 100 points – with one point given for extra credit taking a 89% B and turning it into a 90% A. Grammatical errors, spelling errors etc are not factual errors.

Extra credit projects must be requested to the professor in advance in order to get the credit. Extra credit projects must be finished and presented in a timely and professional manner. Projects will not exceed 5 points in value. Extra credit projects will not be given later than two weeks before the final.

# LAB1: Windows Core/Active Directory

**Student Learning Outcomes satisfied:**

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[ ]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[ ]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[ ]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[ ]  Configure Windows to securely communicate on a Windows network

[ ]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

**Purpose:**

This lab is designed to take students through the process of minimizing system overhead, services and applications.

In this lab, students will be using online and provided information to install a minimal version of Windows 2008 server.

Once the system is installed, the following must function:

 Remote Desktop (RDP)

 Active Directory

**Software Requirements**

Windows 2008r2 server CORE

**Student Materials**

**Student Deliverables**

1. **Lab Report including:**
	1. **Screenshots of key points during the install**
	2. **Screenshots of setup of Active Directory and unattended setup file**
	3. **Setup of two domain user accounts (One Domain User, one Domain Administrator)**
	4. **How Remote Desktop was enabled and a screenshot of the RDP console after logged in from a remote machine.**
2. **A successfully installed Windows 2008 CORE server with the above RDP functionality enabled and working**

**Assessment:**

# LAB 1:Windows Core Evaluation Criteria

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **POINTS** | **POINTS EARNED** | **COMMENTS** |
| **Overall look and feel** |
| **Title Page** | 3 |  | Title page neat, clean, includes lab # and lab title, Student’s name, date, e-mail address, class and section number are included. |
| **Table of Contents** | 2 |  |  |
| **Executive Summary** | 5 |  | System meets all the configuration requirements from the template ([www.cisecurity.org](http://www.cisecurity.org))  |
| **Professional Appearance** | 5 |  | Readability, organization |
| **Header** | 2 |  | – Lab Title |
| **Footer**  | 2 |  | – page, course # and student name |
| **Numbered & Labeled Figures** | 6 |  | Labeled Tables, screenshots & Diagrams |
|  |  |  |  |
| **Content** |
| **Body Content** | 15 |  | Clear and well organized point by point description of the install and how RDP was setup. |
| **System Configuration** |
| **Proper function of server** | 15 |  | Remote Desktop works properly. Computer has network connectivity. Active Directory functioning and installed. |
| **Final result** | 5 |  | Screenshot of RDP working from a remote computerScreenshot of the commands used to create user accounts |
| Total: | 60 |  | Final grade will be divided by 6 to yield the number of points for the lab grade (example, 57 points / 6 = 9.5 points) |

# LAB2: Group Policy

Note – students must be able to set up a Windows 2008 server as a domain controller while performing this lab. A quick refresher can be obtained at: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/domcntrl.mspx

We will **not** be setting up a DHCP server in this lab.

**Student Learning Outcomes satisfied:**

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[ ]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[ ]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[ ]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

**Purpose:**

This lab is designed to take students through the steps of configuring and applying group policy on a Windows Active Directory domain. Students will learn that policies have specific places where they should be applied. Linking policies, creating exceptions and organizing policies will also be learned.

Specific policies will include:

* Password policy (domain)
* Authentication and secure communication policy
* Firewall policy
* Creating exceptions as needed

**Software Requirements**

Windows 2008r2 server configured as a Domain Controller (from the previous lab)

Microsoft Remote Server Administration Tools for Windows 7 http://www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d&displaylang=en

**Student Materials**

**Student Deliverables**

1. **Lab Report**
2. **A successfully configured Windows 2008 Domain Controller with all required security policies in place**
3. **GPMC reports for Default Domain Policy, Screen Lock Policy and the group policy results report for a test user.**

**Assessment:**

# LAB 2 Evaluation Criteria

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPONENT** | **POINTS** | **POINTS EARNED** | **COMMENTS** |
| **Overall look and feel** |
| **Title Page** | 3 |  | Title page neat, clean, includes lab # and lab title, Student’s name, date, e-mail address, class and section number are included. |
| **Table of Contents** | 2 |  |  |
| **Executive Summary** | 5 |  |  |
| **Professional Appearance** | 5 |  | Binding, print quality, cover |
| **Header** | 2 |  | – Lab Title |
| **Footer**  | 2 |  | – page, course # and student name |
| **Section Headings** | 2 |  |  |
| **Numbered & Labeled Figures** | 2 |  | Tables & Diagrams |
| **Numbered Pages** | 2 |  |  |
| **Content** |
| **Body Content** | 15 |  | Clear and well organized point by point description of the actions takenEach component should have its own section. |
| **Discussion** | 10 |  | Discussion section has correct findings and appropriate answers to questions asked at the end of the lab |
| **System Configuration** |
| **Proper function of server** | 5 |  | The following policies are in place and meet reasonable expectations:* Password policy components
* Authentication and secure communication components
* Block execution policy component
* Lock Workstation
* Creating exceptions as needed
 |
| **GPMC resultant policy correct** | 5 |  | GPMC reports for ‘test’ indicates proper settings for each policy, and the group policy results report for the test user is included. |
| Total: | 60 |  | Final grade will be divided by 6 to yield the number of points for the lab grade (example, 57 points / 6 = 9.5 points) |

Final LAB

## Outcomes

**Student Learning Outcomes satisfied:**

[x]  Be familiar with the various security technologies built into with Windows server operating system

[x]  Securely install and configure new Windows Machines on a network.

[x]  Develop and implement Windows Group Policy Objects (GPO) and Network Access Protection (NAP) to minimize system weaknesses and secure network communications

[x]  Plan, organize and implement a patch management system to keep the Windows Enterprise up to date with patches.

[x]  Scan for, Identify and catalog Windows security weaknesses and remediate vulnerabilities.

[x]  Configure Windows to securely communicate on a Windows network

[x]  Configure, Implement, Secure and troubleshoot a centralized Windows auditing system.

## Description/Requirements:

The final lab will be administered using the Blackboard assessment tool during the last class. The final will be open book and open notes. The final will have a three hour time limit. ***While the final is a Lab, the scoring component will be in a question and answer format within Blackboard/Blackboard.***

## Grading/Points Possible:

* The Final lab will be worth 30 points of the overall course grade.
* The final lab must be completed in 3 hours
* Please see the course grading policy for additional details on the grading of late assignments.

Stevenson University College Policies

## Academic Honesty Penalty

Any attempt to commit cheating, plagiarism, unauthorized assistance, fabrication, multiple submissions, or other violations as defined in the Stevenson University academic Honesty Policy constitutes academic dishonesty. A violation of academic honesty is considered a serious offense by the college administration. Penalties include loss of credit for the assignment or failure of the course at the discretion of the instructor. Violations may also lead to dismissal from the program or college at the discretion of the Associate Dean for Academic Support Services. Any attempt to commit the following offenses constitutes academic dishonesty.

### Cheating:

Using unauthorized material to complete a test, quiz, examination, or assignment. Cheating includes, but is not limited to, copying from other students, relying upon aids or notes during a test, or consulting outside sources without the instructor's permission. Giving unauthorized assistance to other students also constitutes cheating.

### Plagiarism:

Representing the words, ideas, research, or works of another as one’s own.  Plagiarism can involve submitting work prepared entirely or in part by another person or commercial service or borrowing material as direct quotation, partial quotation, or paraphrase from published or unpublished sources without proper acknowledgement.  Students must document all print, online, and oral sources they use to complete assignments.

### Unauthorized Assistance:

Preparing an assignment with the help of another student or allowing another person, such as a tutor, to alter or revise an assignment beyond the scope of collaboration the instructor has defined.

### Fabrication:

Presenting false data, sources, or research results for academic credit.

### Multiple Submission:

Presenting the same work, in whole or in part, for credit in more than one course without the explicit permission of all interested instructors.

### Other Violations:

Including, but not limited to, lying, forgery, bribery, damaging or stealing college or another’s property, physically abusing another person, or verbally threatening another.

**Any violation of the Academic Honesty Policy may result in an ‘F’ for the assignment or an ‘F’ for the course at the discretion of the instructor. This penalty could be changed to dismissal from the college by higher authorities.**

**A violation of this policy will result in a grading penalty to be determined at the discretion of the instructor**

(See www. <http://www.VJC.edu/academics/index.aspx?id=3110> for the full Academic Honesty Policy.)

## Students with Disabilities

Consult the Stevenson University Catalog.

## Network Security Agreement

All components of the Stevenson University Network Security Agreement will be enforced in this class. Failure to abide by this agreement will result in the loss of your access to the college computer facilities. The loss of computer access will not excuse you from completing any of the course requirements. Class assignments, announcements, and other materials may be distributed via e-mail, the Stevenson University network or the Stevenson University Blackboard during the semester. It is the responsibility of the student to check their Stevenson University e-mail account and Blackboard each school day, to check the class network directory, and to report to the instructor any problem with the campus telecommunications system.

## Classroom PC Acceptable Use Policy

During class time, the classroom PC is to be used for class activities only as directed by the instructor. Any other use is in violation of the Classroom PC Acceptable Use Policy.

* The use of cell phones, PDAs or other electronic devices will not be allowed during class time. These devices are to be turned off before the start of each class.
* Monitors are to be turned off at the start of class unless otherwise directed by the instructor.
* The use of Instant Messaging (IM) or email is prohibited during class.

### Penalty:

Failure of a student to follow the Classroom PC Acceptable Use Policy may result in the student being asked to leave the class and / or the subtraction of points from the student’s final average.

**The instructor is in charge of the classroom. Refusal of any request to turn off monitors, cell phones, or any other equipment detailed in this policy will result in a grading penalty the range of which is at the discretion of the instructor**.

**A violation of this policy will result in a grading penalty to be determined at the discretion of the instructor**

# REFERENCE MATERIALS AND RESOURCES

**SOFTWARE:**

Sysinternals autorunsc utility (<http://www.sysinternals.com/Utilities/autoruns.html>)

Foundstone Fport utility ([www.foundstone.com/knowledge/proddesc/fport.html](http://www.foundstone.com/knowledge/proddesc/fport.html))

**DOCUMENTATION:**

|  |  |
| --- | --- |
| **RESOURCES** | **URL** |
| Step-by-Step Guides for Windows Server 2008.  | <http://www.microsoft.com/downloads/details.aspx?FamilyID=518d870c-fa3e-4f6a-97f5-acaf31de6dce&displaylang=en>  |
| Windows Server 2008 Security Guide | <http://technet.microsoft.com/en-us/library/cc264463.aspx>  |
| Threats and Countermeasures Guide | <http://go.microsoft.com/fwlink/?LinkId=15159> |
| [Step-by-Step Guide to Getting Started with Microsoft Windows Server Update Services](http://www.microsoft.com/downloads/details.aspx?FamilyId=3BA03939-A5A9-407B-A4B0-1290BA5182F8&displaylang=en) | <http://www.microsoft.com/windowsserversystem/updateservices/downloads/WSUSSP1.mspx> |
| Group Policy Resource site | <http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx>  |
| Windows 2008 Security Event Descriptions  | <http://support.microsoft.com/kb/947226>  |
|  |  |
| Kiwi Syslog Daemon manual  | <http://www.kiwitools.com/downloads/syslog/Syslogd.pdf>  |
| Varonis | <http://www.varonis.com/>  |
| Auditing and Compliance in Windows Server 2008 | <http://technet.microsoft.com/en-us/magazine/cc194392.aspx>  |

**MISC:**

Online Research Resources

SITE: NSA guides

PURPOSE: NSA produced guides on securing Windows 2003

URL: <http://www.nsa.gov/snac/downloads_all.cfm?MenuID=scg10.3.1>

SITE: SANS Reading Room

PURPOSE: various security papers on a variety of subjects, including Windows.

URL: <http://www.sans.org/reading_room/>

SITE: Microsoft Security Home Page

PURPOSE: portal to all things dealing with security from Microsoft

URL: <http://www.microsoft.com/security>

SITE: SYSLOG Client configs for Windows/Non-UNIX

PURPOSE: Help and hints for implementing a SYSLOG infrastructure with Windows systems.

URL: <http://www.loganalysis.org/> - click on “Windows to syslog” link.

SITE: Microsoft GPMC web page (documentation and software)

PURPOSE: streamline and organize Group policy for Active Directory. Also enables reporting

URL: <http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>

SITE: Windows Security Log Encyclopedia

PURPOSE: Description of various Windows security log events and their meaning

URL: <http://www.ultimatewindowssecurity.com/encyclopedia.html>

SITE: Microsoft Technet

PURPOSE: Primary site for Windows documentation

URL: <http://technet.microsoft.com>

SITE: The Center for Internet Security

PURPOSE: resource for security templates and a security scoring tool.

URL: <http://www.cisecurity.org>

# Course Bibliography

Roberta Bragg, **Windows Server 2003 Security : A Technical Reference,** Addison-Wesley Professional, 2005, **ISBN:** 0321305019

Mike Danseglio & Robbie Allen, **Windows Server 2003 Security Cookbook,** O'Reilly Media, 2005, **ISBN:** 0596007531

Derek Melber, **Auditing Security and Controls of Windows® Server 2000 and Windows® Server 2003, T**he Institute of Internal Auditors Research Foundation, 2005, **ISBN:** 0894135643

Mike Danseglio, **Securing Windows Server 2003,** O'Reilly Media, 2004, **ISBN:** 0596006853