PELLISSIPPI STATE TECHNICAL COMMUNITY COLLEGE
MASTER SYLLABUS

CIW Server Administrator
WEB 2601

Class Hours: 3 Credit Hours: 3
Laboratory Hours: 0.0 Revised: Spring 08

NOTE: This course is not designed for transfer credit.

Catalog Course Description:

This course focuses on server and network administration tasks and tools implemented by IT professionals. Students will learn to configure and manage corporate Internet and intranet infrastructure; monitor Web, FTP, news, and mail servers; and figure and deploy e-business solutions servers. CIW Server Administrators manage and tune corporate e-business solutions and infrastructure including Web, FTP, news and mail servers, for midsize to large businesses.

Entry Level Standards:

Students taking this course should be proficient in Windows XP

Prerequisites:

WEB 2200

Co-requisites:

WEB 2691

Textbook(s) and Other Course Materials:


3) Hardware and Software Requirements:
   - Pentium III/750 MHz processing speed
   - 256 MB RAM
   - Monitor capable of at least 800 x 600 resolution
   - CD-ROM drive
   - 56 kbps modem with Internet access (high speed such as cable modem or DSL recommended if possible)
   - Operating System: Windows XP
   - Basic text editor
   - FTP or Telnet software

I. Week/Unit/Topic Basis:

1 Lesson 1: IT Systems and Services Overview.
   Lesson 2: Internet System Installation and Configuration Issues
   Assignment 1
II. Course Objectives*

A. Explain common IT services, focusing on hardware platforms and frequently used operating systems. (I)
B. Apply TCP/IP configuration parameters, and Windows 2000, and Linux system configuration with static IP addresses. (I, IV)

C. Apply user access levels, password policies, and permissions based on standard practice and procedures. (I, II)

D. Describe management of users in Windows 2000 and Linux. (I, IV)

E. Explain Domain Name System (DNS) in Windows 2000 and Linux. (I, II)

F. Use name resolution options for LANs and WANs, including the Windows Internet Naming Service (WINS) and Samba. (II)

G. Use Internet services including FTP and Telnet, and control of access to these services. (II, IV)

H. Utilize web servers, including Microsoft IIS and Apache Server. (II, IV)

I. Perform advanced Web server administration tasks. (II, IV)

J. Utilize user-based access to Web servers. (II, IV)

K. Explain the limitation of access based on IP addresses. (II, IV)

L. Describe the functionality of a Web server, including Perl configuration and additional services. (II, IV)

M. Apply web server connection to a database via Open Database Connectivity (ODBC). (II, IV)

N. Apply configuration and management of streaming media servers. (II, IV)

O. Utilize Secure Sockets Layer (SSL) transactions. (II, IV)

P. Apply management of news servers. (II, IV)

Q. Describe configuration and management of SMTP, IMAP and POP3 e-mail servers. (II, IV)

R. Perform server and service log analysis. (II, IV)

S. Explain configuration and management of proxy servers and Internet servers. (II, IV)

T. Perform system performance evaluation. (II, IV)

U. Describe internal and external security risks. (II, IV)

*Roman numerals after course objectives reference goals of the WEB program.

III. Instructional Processes*:

Students will:

1. Explain the server and network administration tasks and tools required by IT professionals. *(Technological literacy outcome)*

2. Identify the current direction and application of server administration. *(Technological literacy outcome)*
3. Identify the differences between e-business solutions and infrastructure tools used in midsize to large businesses. (*Technological literacy outcome*)
4. Monitor FTP, news and mail servers, and Web servers. (*Technological literacy outcome*)
5. Configure and deploy e-business solutions servers. (*Active Learning Strategies*)
6. Use research activities to promote independent thinking. (*Active Learning Strategies*)
7. Use software tools and web development skills to administer web sites that are functional and efficient. (*Active Learning Strategies*)

*Strategies and outcomes listed after instructional processes reference TBR's goals for strengthening general education knowledge and skills, connecting course work to experiences beyond the classroom, and encouraging students to take active and responsible roles in the educational process.

**IV. Expectations for Student Performance***:

Upon successful completion of this course, the student should be able to:

1. List the services offered by IT departments. (A)
2. Identify backbone and mission-critical services offered by IT departments. (A)
3. Discuss the concepts of system maintenance, including fault tolerance, server optimization, and backup. (A)
4. Identify common hardware platforms. (A)
5. Describe capabilities of various platform components, including multiple CPUs, I/O issues, and system memory. (A)
6. Define bandwidth and throughput (A)
7. Identify common network operating systems (A)
8. Determine the ideal operating system for a given environment. (A)
9. Discuss system installation issues. (A)
10. List key TCP/IP configuration parameters. (B)
11. Add NICs in Windows 2000 and Linux (B)
12. Configure Windows 2000 with static IP addresses. (B)
13. Configure Linux with static IP addresses. (B)
14. Describe how DHCP works. (B)
15. Define authentication. (C)
16. Explain the share-level and user-level access security models. (C)
17. Identify the purposes and functions of logon accounts, groups, and passwords. (C)
18. Create a network password policy using standard practices and procedures. (C)
19. Discuss permissions issues. (C)
20. Describe the relationship between permissions and user profiles (C)
21. Use administrative utilities for specific networks and operating systems (C)
22. Identify the permissions needed to add, delete, or modify user accounts. (D)
23. Identify the purpose of the Windows 2000 Security Accounts Manager. (D)
24. Enforce system wide policies, including account lockout settings, password rules, and password aging. (D)
25. Convert a FAT drive to NTFS. (D)
26. Enable auditing in Windows 2000 Server. (D)
27. View local and remote events in Event Viewer. (D)
28. Manage file and directory ownership. (D)
29. Manage user rights. (D)
30. Enable custom user settings, such as specifying home directories, logon scripts, and dial-in access. (D)
31. Identify accounts used by Windows 2000 services. (D)
32. Create new accounts on Linux systems. (D)
33. Set password-aging policies on Linux systems. (D)
34. Set account policies in Linux. (D)
35. View user accounts used by system daemons. (D)
36. Explain run levels. (D)
37. Use the ntsysv and chkconfig commands. (D)
38. Explain the Domain Name System (DNS). (E)
39. Identify DNS components, including zones, name server types, and resolvers. (E)
40. List and create the common DNS record types, including A, NS, and CNAME. (E)
41. Define reverse DNS lookup. (E)
42. Implement DNS in Windows 2000 and Linux. (E)
43. Deploy Dynamic DNS (DDNS). (E)
44. Configure caching servers and forwarders. (E)
45. Use nslookup and additional troubleshooting tools. (E)
46. Explain the basics of NetBIOS, including the NetBIOS naming convention. (F)
47. Identify additional name resolution options for LANs and WANs. (F)
48. Implement and manage WINS. (F)
49. Use Samba to create a WINS server in UNIX. (F)
50. Configure a UNIX system as a WINS client. (F)
51. Configure Samba systems to use Windows 2000 authentication. (F)
52. Create and manage shares using Samba. (F)
53. Deploy user-level and anonymous FTP access in Windows 2000 and Linux. (G)
54. Describe standard and passive FTP. (G)
55. Configure Telnet for Windows 2000 and Linux. (G)
56. Configure finger in Linux. (G)
57. Control access to Linux services. (G)
58. Identify foundational services, including DNS, WINS, and Samba. (H)
59. List mission-critical services, including Web servers, databases, e-commerce servers, news servers, streaming media servers, e-mail servers, and proxy servers. (H)
60. Discuss system maintenance and logging. (I)
61. Describe performance monitoring and server optimization issues. (I)
62. Explain the importance of implementing security features for your servers. (I)
63. Identify the basic functions of a Web server. (I)
64. Explain how a Web server identifies file types. (I)
65. Customize the server root directories. (I)
66. Redirect URLs and add default document types. (I)
67. Enable user-based authentication for the Web server. (J)
68. Control access to a Web server based on IP address. (K)
69. Enable HTML administration for IIS 5.0. (L)
70. Create virtual servers and directories (i.e. aliases) in IIS and Apache Server. (L)
71. Implement common e-commerce elements, including databases and streaming media services. (M, N)
72. Identify key HTTP error messages. (N)
73. Create a custom HTTP error message in IIS 5.0 (N)
74. Explain how Web servers and clients and clients use MIME. (N)
75. Describe how Web applications work with IIS 5.0. (N)
76. Execute Active Server Pages (ASP) and CGI scripts in an e-commerce setting. (N)
77. Connect a Web site to a database using a Web application. (N)
78. Install, configure, and test a streaming media server. (N)
79. Describe the functions of Secure Sockets Layer (SSL). (O)
80. Identify the SSL handshake process. (O)
81. Use the Internet Services Manager to generate an SSL certificate request. (O)
82. Deploy the Certificate Authority snap-in to sign certificate requests. (O)
83. Configure IIS 5.0 to use SSL. (O)
84. Create newsgroups in both Windows 2000 and Linux. (P)
85. Configure newsgroup expiration policies. (P)
86. Control client access to a news server through IP access filtering and user-based authentications. (P)
87. Describe the process of sending an e-mail message. (Q)
88. Explain key e-mail server concepts, including forwarding, masquerading, and aliasing. (Q)
89. Describe the functions of e-mail protocols such as SMTP, POP3, IMAP, and LDAP. (Q)
90. Identify the purpose and usefulness of MX records. (Q)
91. Discuss DNS as it applies to e-mail servers. (Q)
92. Install an e-mail server in Windows 2000. (Q)
93. Manage a Web-based e-mail service. (Q)
94. Configure an e-mail server to filter content. (Q)
95. Display a list server. (Q)
96. Explain the benefits of a proxy server. (S)
97. Differentiate between public and private IP addresses. (S)
98. Install and configure web-based and SMTP-based proxy servers. (S)
99. Explain the need for logging activity generated by servers and services. (R)
100. Configure Web server logs in IIS, Apache Server, and ftpd. (R)
101. Identify the need to check DNS and e-mail logs. (R)
102. View information from a Web server log files using commercial log analysis software. (R)
103. Explain the need for server monitoring and optimization. (T)
104. Utilize tools when monitoring and optimizing servers. (T)
105. Identify key Internet server elements to monitor. (T)
106. Adjust Internet server settings to meet expected workload. (T)
107. Identify ways to create fault tolerance in a network host. (U)
108. Explain the concept of offsite storage. (U)
109. Implement procedures for disaster assessment. (U)
110. Follow a data-recovery strategy. (U)
111. Implement recovery procedures to repair corrupted data. (U)
112. Identify vulnerabilities commonly found in various operating systems. (U)
113. List the steps to counteract operating system weaknesses. (U)
114. Define firewall and intrusion detections concepts. (U)
115. Discuss the effects of security measures on employees and system hosts. (U)
116. Recognize security breaches. (U)

*Letters after performance expectations reference the course objectives listed above.

V. Evaluation:

A. Assignments: 50%
   Students will have weekly assignments to complete.

B. Exams: 40%
   Students will complete four comprehensive quizzes that will cover the course text.

C. Field Work:
   N/A

D. Other Evaluation Methods: 10%
   Online Communication Tools: 10% of grade

E. Grading Scale:

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>90-100</td>
<td>A</td>
</tr>
<tr>
<td>80-89</td>
<td>B</td>
</tr>
<tr>
<td>70-79</td>
<td>C</td>
</tr>
<tr>
<td>60-69</td>
<td>D</td>
</tr>
<tr>
<td>below 60</td>
<td>F</td>
</tr>
</tbody>
</table>

VI. Policies:
A. Attendance Policy:

Pellissippi State Technical Community College expects students to attend all scheduled instructional activities. As a minimum, students in all courses must be present for at least 75 percent of their scheduled class and laboratory meetings in order to receive credit for the course (Pellissippi State Catalog). Individual departments, programs, or disciplines, with the approval of the vice president of Academic and Student Affairs, may have requirements that are more stringent.

B. Academic Dishonesty:

Plagiarism, cheating and other forms of academic misconduct are prohibited. A student guilty of academic misconduct, either directly or indirectly through participation or assistance, is immediately responsible to the instructor of the class. In addition to other possible disciplinary sanctions that may be imposed through the regular Pellissippi State procedures as a result of academic misconduct, the instructor has the authority to assign an F or a zero for the exercise or examination or to assign an F in the course. (Pellissippi State Catalog)

C. Accommodations for disabilities:

If you need accommodations because of a disability, if you have emergency medical information to share, or if you need special arrangements in case the building must be evacuated, please inform the instructor immediately. Please see the instructor privately after class or in his/her office. Students must present a current accommodation plan from a staff member in Services for Students with Disabilities (SSWD) in order to receive accommodations in this course. Services for Students with Disabilities may be contacted by going to Goins 127 or 131 or by phone: 694-6751(Voice/TTY) or 539-7153.

D. Other Policies:

Use of Equipment:
Any act of misuse, vandalism, malicious or unwarranted damage or destruction, defacing, disfiguring, or unauthorized use of property/equipment belonging to Pellissippi State is subject to disciplinary sanction.

Hardware/Software Requirements for this Course

IBM-type criteria:

Hardware:

- Intel Pentium 4, Intel Centrino, Intel Xeon, or Intel Core Duo (or compatible) processor.
- Microsoft Windows XP with Service Pack 2 or Windows Vista Home Premium, Business, Ultimate or Enterprise (certified for 32-bit editions)
- 1 GB of RAM
- 5 GB of available hard-disk space
- 1024 x 768 monitor resolution with 16-bit video card
- CD-ROM drive (DVD preferred)
- High-speed Internet connection such as cable modem or DSL recommended, if possible
- Speakers

Software:
• Internet Explorer 6.0 (or higher) with Outlook Express
• Macromedia Shockwave and Flash players. Download free from http://www.macromedia.com/downloads/
• Adobe Acrobat Reader 6.0 or better. Download free from http://www.adobe.com/support/downloads/main.html
• OPTIONAL: Netscape 7.0 (full installation)

Macintosh criteria:

Hardware:
• PowerPC G4 or G5 or multicore Intel processor
• Mac OS X v.10.4.8
• 1 GB of RAM
• 7 GB of available hard-disk space space
• 1024 x 768 monitor resolution with 16-bit video card
• CD-ROM (DVD preferred)
• High-speed Internet connection such as cable modem or DSL recommended, if possible
• Speakers

Software:
• QuickTime 7.0.4 or better
• Adobe Acrobat Reader 6 or better. Download free from http://www.adobe.com/support/downloads/main.html
• Macromedia Shockwave and Flash players. Download free from http://www.macromedia.com/downloads/

FOR CIW Courses: CD-ROM. Each coursebook includes a supplemental CD-ROM with files that are referenced and used in the course. The labs will refer you to the CD and you will access these and use the files in the course.