IT 293-501 Fall 2015

Guide to Hardware: Managing, Maintaining, and Troubleshooting

Instructor: John E. Abrams **Office:** Office CSS Offices

Office Hours: Immediately after class for fourty-five minutes **E-mail:** jeabrams@unm.edu

Phone: 925-8700 - **You can leave a message** **Classroom:** B123a

Course Title Number and Section: Topics Cyber Security 293-501

Class Times: Tuesday and Thursday 4:30 to 5:45 – 16 weeks

Semester Date and Duration: Start date 01/17/2017 - End date 05/17/2017

CRN: 57114

Prerequisites: IT 125,131

Course Description: The purpose of this course is to prepare students to take and pass the CompTIA national Security+ Technician certification test. Students will learn concepts, terminology, tools, and best practice for securing IT systems and networks. This includes Access control, Cryptology, Policy & Procedure, Defense, Assessment and Audit requirements. Students will also practice proper safety procedures, perform preventative configuration. Installation and operation of security software. In addition, students will configure, diagnose, and troubleshoot network and system security settings. Finally, students will learn and apply industry accepted skills and security standards.

Textbook: Subscription to LabSim SecurityPro http://testout.com

Course Objectives

Students will be able to identify, explain, define and deTuestrate the step-by-step approach for the application of security practices. Beginning steps toward CompTIA's Security+ 220-701 and 220-702 Exam objectives.

Specific topic coverage includes:

- Access Control & ID Management
- Cryptography
- Awareness Policy & Procedure
- Physical Security
- Perimeter defense
- Network defense
- Host defense
- Application defense
- Data Defense

Web Site

Supplementary information for the course is available on the Learn Blackboard Course (URL http://learn.unm.edu). The Web site contains class notes, PowerPoint slides, class announcements, the course syllabus, test dates, and other information for the course.

Week	Course day	Topics/Activity	Items Readings and Exams Due
1 Tue	1 1/17	Welcome and Introduction Review Syllabus/ E-mail accounts LabSim Familiarization Section 1.0 Security overview	Buy storage device and TestOut Key Code/ Enroll in TestOut/LabSim **Course:** TestOut Security Pro
Thur	2	Section 1.0 Computing Overview Working with LabSim LabSim Familiarization	,
2 Tue	3	Section 2.0 Access control Authentication, Authorization, Access control Best Practice, Active Directory, Windows domain Users & Groups. Group Policy	
		Section 2.7 Linux Users, Groups, User security	
	4	Hardening systems	
3 Tue	5	Labor day	
	6	Section 3.0 Cryptography	
4 Tue	7	Section 4.0 Security Policy, Network planning, risk management	
	8	Section 5.0 Physical Security	
5 Tue	9	Section 6.0 Network Layer Protocol Review	
	10	**CHAPTERS 1-5 EXAM** **(Online Take-home Opens Today)** Network Layer Protocol Review	
6 Tue	11	Section 7.0 Network Devices	
	12	Section 8.0 Malware	
7 Tue	13	Section 9.0 Web Attacks	
	14	Section 10.0 Redundancy	
8 Tue	15	Backup/Restore	
	16	Secure protocols	
9 Tue	17	Cloud Computing	
	18	Section 11.0 Vulnerability Assessment, ,	
10 Tue	19	Log management, Audit	
	20	Protocol analyzers Tools Lab	**Complete Missing Assignments to date**
11 Tue	21	Protocol analyzers Tools Lab	
	22	**CHAPTERS 6-11 EXAM** **(Online Take-Home Opens Today)** Section 12.0 Security Overview	

12 Tue	**23**	Penetration Testing Tools Lab	
	24	Penetration Testing Tools Lab	
13 Tue	**25**	Penetration Testing Tools Lab	Certification Practice Exam (Labs)
	26	SecurityPro Certification Practice Exam (Labs	**Complete all sections including missing assignments**
14 Tue	**27**	**Make-Up Day**	
	28	**1. Student Presentations for Final Review**	
15 Tue	**29**	**2. Student Presentations for Final Review**	
	30	**3. Student Presentations for Final Review** **Final Review**	
16 Tue	**31**	**Final Review**	
	32	**Security Pro Exam FINAL**	**In Class Final Exam**

E-Mail All students must have a UNM e-mail account. If you have any questions about the course or need assistance, please contact me in person or by telephone during office hours; or by e-mail at any time. All quizzes and tests are going to be taken using LabSim. Grades will be posted to Blackboard weekly.

UNM Email/Black Board Learn Access

UNM-Valencia students must have a UNM Net ID which can be created by going to: http://it.unm.edu/accounts/.

The UNM Net ID will give you access to the computer labs on campus, blackboard learn and UNM Email.

Grading and Evaluation Criteria

80% of the grade is based on Assessments in Lab Sim.

15% of the grade is based on completion of hands on activities that will be assigned as part of class lab sessions.

5% of the grade will be based on a presentation based on an in class presentation based on scenarios and security issues that professionals encounter daily in a typical organization.

Both midterm and final exams will be counted in total points earned and the total value of all points earned will determine final percentage toward final grade.

These percentages will be used to assign final grades:

A+ = 100–98	A = 97–94	A- = 93–90	B+ = 89–87	B = 86–84
B- = 83–80	C+ = 79–77	C = 76–74	C- = 73–70	D+ = 69–67
D = 66–64	D- = 63–60	F = 59–0		

Computer Lab Responsibility:

Please be advised that use of computer labs on UNM properties is governed by "Policy 2500: Acceptable Computer Use"

Which can be found at http://policy.unm.edu/university-policies/2000/2500.html. Food and drink are also prohibited in any computer lab on campus. Anyone violating these policies is subject to possible suspension and loss of computer lab privileges.

Academic Integrity:

Having academic integrity is paramount to your success in any class. Plagiarism or cheating is not tolerated. Any instance of this will result in a grade of zero for that assignment. Here is the link to the UNM Academic Dishonesty Policy: https://policy.unm.edu/regents-policies/section-4/4-8.html. The policy states:

Each student is expected to maintain the highest standards of honesty and integrity in academic and professional matters. The University reserves the right to take disciplinary action, up to and including dismissal, against any student who is found guilty of academic dishonesty or who otherwise fails to meet the expected standards. Any student judged to have engaged in academic dishonesty in course work may receive a reduced or failing grade for the work in question and/or for the course.

Academic Dishonesty is defined as:

"Academic dishonesty" includes, but is not limited to, dishonesty in quizzes, tests, or assignments; claiming credit for work not done or done by others; hindering the academic work of other students; misrepresenting academic or professional qualifications within or without the University; and nondisclosure or misrepresentation in filling out applications or other University records.

If you have a documented disability

The Equal Access Services office will provide me with a letter outlining your accommodations. I will then discuss the accommodations with you to determine the best learning environment. If you feel that you need accommodations, but have not documented your disability, please contact Jeanne Lujan, the coordinator for Equal Access Services at 925-8910 or jmlujan@unm.edu.

In an effort to meet obligations under Title IX
UNM faculty, Teaching Assistants, and Graduate Assistants are considered "responsible employees" by the Department of Education
(See page 15 - http://www2.ed.gov/about/offices/list/ocr/docs/qa-201404-title-ix.pdf).
This designation requires that any report of gender discrimination which includes sexual harassment, sexual misconduct and sexual violence made to a faculty member, TA, or GA must be reported to the Title IX Coordinator at the Office of Equal Opportunity (oeo.unm.edu). For more information on the campus policy regarding sexual misconduct,
see: https://policy.unm.edu/university-policies/2000/2740.html.

The total time for the LabSim Security Pro course is approximately 91 hours and 35 minutes. The time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo times
- Approximate time to read the text lesson (the length of each text lesson is taken into consideration)
- Simulations (5 minutes assigned per simulation)
- Questions (1 minute per question)

The breakdown for this course is as follows:

Module	Sections	Time	Total	HR:MM
1.0 Introduction				
	1.1 Security Overview	70		
	1.2 Using the Simulator	25	95	1:35
2.0 Access Control and Identity Management				
	2.1 Access Control Models	30		
	2.2 Authentication	60		
	2.3 Authorization	30		
	2.4 Access Control Best Practices	30		
	2.5 Active Directory Overview	30		
	2.6 Windows Domain Users and Groups	50		
	2.7 Linux Users	70		
	2.8 Linux Groups	20		
	2.9 Linux User Security	25		
	2.10 Group Policy Overview	35		

2.11 Hardening Authentication 1	90		
2.12 Hardening Authentication 2	30		
2.13 Remote Access	35		
2.14 Network Authentication	70		
2.15 Identity Management	20	625	10:25
3.0 Cryptography			
3.1 Cryptography	45		
3.2 Hashing	35		
3.3 Symmetric Encryption	35		
3.4 Asymmetric Encryption	25		
3.5 Public Key Infrastructure (PKI)	70		
3.6 Cryptography Implementations	40	250	4:10
4.0 Policies, Procedures, and Awareness			
4.1 Security Policies	80		
4.2 Manageable Network Plan	35		
4.3 Business Continuity	20		
4.4 Risk Management	30		
4.5 Incident Response	65		
4.6 Social Engineering	55		
4.7 Certification and Accreditation	40		
4.8 Development	35		
4.9 Employee Management	40		
4.10 Third-Party Integration	20	420	7:00
5.0 Physical Security			
5.1 Physical Security	50		
5.2 Hardware Security	20		
5.3 Environmental Controls	45		
5.4 Mobile Devices	40		
5.5 Mobile Device Security Enforcement	40		
5.6 Telephony	25	220	3:40
6.0 Networking			
6.1 Networking Layer Protocol Review	65		
6.2 Transport Layer Protocol Review	35		
6.3 Perimeter Attacks 1	50		
6.4 Perimeter Attacks 2	50		
6.5 Security Appliances	35		
6.6 Demilitarized Zones (DMZ)	30		
6.7 Firewalls	40		

6.8 Network Address Translation (NAT)	30		
6.9 Virtual Private Networks (VPN)	40		
6.10 Web Threat Protection	25		
6.11 Network Access Control (NAC)	45		
6.12 Wireless Overview	60		
6.13 Wireless Attacks	50		
6.14 Wireless Defenses	80	635	10:35

7.0 Network Defenses			
7.1 Network Devices	15		
7.2 Network Device Vulnerabilities	20		
7.3 Switch Attacks	10		
7.4 Router Security	15		
7.5 Switch Security	90		
7.6 Intrusion Detection and Prevention	50		
7.7 SAN Security	30	230	3:50

8.0 Host Defenses			
8.1 Malware	75		
8.2 Password Attacks	20		
8.3 Windows System Hardening	105		
8.4 Hardening Enforcement	35		
8.5 File Server Security	50		
8.6 Linux Host Security	20		
8.7 Static Environment Security	10	315	5:15

9.0 Application Defenses			
9.1 Web Application Attacks	75		
9.2 Internet Browsers	105		
9.3 E-mail	45		
9.4 Network Applications	25		
9.5 Virtualization	55		
9.6 Application Development	75	380	6:20

10.0 Data Defenses			
10.1 Redundancy	65		
10.2 Backup and Restore	55		
10.3 File Encryption	75		
10.4 Secure Protocols	75		
10.5 Cloud Computing	30	300	5:00

11.0 Assessments and Audits			
11.1 Vulnerability Assessment	85		
11.2 Penetration Testing	30		
11.3 Protocol Analyzers	20		
11.4 Log Management	50		
11.5 Audits	40	225	3:45

Security Pro Practice Exams				
	Domain 1: Access Control and Identity Management (22 sims)	110		
	Domain 2: Policies, Procedures, Awareness (1 sim)	5		
	Domain 3: Physical Security (2 sims)	10		
	Domain 4: Perimeter Defenses (10 sims)	50		
	Domain 5: Network Defenses (7 sims)	35		
	Domain 6: Host Defenses (7 sims)	35		
	Domain 7: Application Defenses (10 sims)	50		
	Domain 8: Data Defenses (6 sims)	30		
	Domain 9: Audits and Assessments (5 sims)	25		
	Security Pro Certification Practice Exam (15 sims)	90	440	7:20
Security+ Practice Exams				
	Domain 1: Network Security (172 questions)	172		
	Domain 2: Compliance and Operational Security (128 questions)	128		
	Domain 3: Threats and Vulnerabilities (178 questions)	178		
	Domain 4: Application, Data and Host Security (70 questions)	70		
	Domain 5: Access Control and Identity Management (98 questions)	98		
	Domain 6: Cryptography (92 questions)	88		
	Security+ Certification Practice Exam (100 questions)	100	834	13:54
SSCP Practice Exams				
	Domain 1: Access Control (60 questions)	60		
	Domain 2: Security Operations & Administration (64 questions)	64		
	Domain 3: Tueitoring and Analysis (21 questions)	21		
	Domain 4: Risk, Response, and Recovery (38 questions)	38		
	Domain 5: Cryptography (90 questions)	90		
	Domain 6: Networks and Communications (68 questions)	68		
	Domain 7: Malicious Code and Attacks (85 questions)	85		
	SSCP Certification Practice Exam (125 questions)	125	551	9:11
		Total Time	**5495**	**91:35**