NETWORK SECURITY

Course Title:	Network Security
Semester:	Spring 2018
Course Code:	CS-411
Credit Hours:	3
Pre-requisite:	Computer Networks
Core/ Elective	Elective
Office Hours:	Tuesday 12.30 – 1.30 PM, Wednesday 12.00 – 2.00 PM
Instructor:	Ibrahim Nadir (Email: ibrahim.nadir@nu.edu.pk, Ext: 257)

Course description:

Network Security is a course on understanding the issues, principals, concepts and mechanisms of information & communication technologies security. It is not a course on Networks, nor on cryptography. But the issues concerning both of them that can be exploited to generate attacks on networks and systems. "Perfect security is a myth" but best selection, implementation and mitigation can achieve a great level of security.

Course objectives:

This course aims to deliver the basic understanding of security of systems and provides in general how security is established between any two end systems. The course focuses on establishing security at all layers of TCP/IP layers discussing the important protocols/frameworks involved in it. The course also provides a little hands-on experience to the students by providing guides towards scanning and penetration testing tools. At the end of the course, an average student should understand what the basic pillars of security are, what cryptography is and what are the basic cryptographic algorithm's working procedure. The student also understands SSL/TLS, IPSec, VPNs and Malware along with authentication systems.

Course Book:

Network Security – Private communication in a public world

Authors: Charlie Kaufman, Mike Speciner and Radia Perlman

Supplement:

Cryptography Network Security: Principal and Practice by William Stallings

Grading Criteria:

Assignments	10%
Quizzes	10%
Class participation and taking initiatives	5%
Two Midterm Exams	30%
Final Exam	45%

Assignments:

You can't cheat assignments, you may discuss them in groups. If found guilty, assignment will be cancelled. No late submissions are allowed.

Quizzes (3-5):

2 announced, 3 surprise quizzes. Best of 3 rule will be applied.

Class participation and taking initiatives:

You may do active participation in class and come up with ideas such as:

- New security protocols or new flavors of existing protocols
- New attack methods
- Doing assignments that are not to be delivered but are given for learning purposes only.

Rules:

- No illegal activities are accepted after learning from this course. You CAN NOT use such knowledge to do unauthorized activity unless you have explicit permission. You are on your own if you did so. I may decide to award you with an F in the course and there will be disciplinary action as well. You are however welcome to try if you are using the knowledge in a sandboxed environment.
- Asking questions regarding grading policies are not going to be entertained. Period!

- Assignments dates will not be extended.

Tentative Lecture Plan:

Lectures	Topics
1,2,3	Introduction to network security. Attacks, Security properties and mechanisms,
4,5,6	Cryptography – Kerchoff’s principal Secret key cryptography, Public Key cryptography, Hashes
7,8,9	Secret Key Cryptography – Stream vs block cipher, DES, IDEA, AES
10,11,12	Mode of operations – ECB, CBC, OFB, CFB
13	Storage Encryption – File encryption, Disk Encryption, TPM
14,15,16	Hashes and message digests – Porperties of Hash functions, Birthday problem, MD2, MD4, MD5, SHA-1, HMAC
17,18,19	Public Key Cryptography – Coprime, Euler Totient function, RSA, Diffie Hellman, ECC, Digital Signatures, El Gamal, DSS
20,21	Public Key Infrastructure
22	Authentication Systems
23	SSL / TLS
24,25	IPSec: AH & ESP
26,27	Malware – Virus, Worm…, Propagation, Detection, Prevention
28	VPN

Piazza link: **http://piazza.com/fast_lahore/spring2018/cs411**

Access code: **cs411**