Network Security (cs6500)

Jan- April 2019

Chester Rebeiro, IIT Madras

Schedule

Quiz and End Sem Schedule **Mid Semester :** 11/3/2019 **EndSem :** (as per academic calendar)	**Grading Policy** MidSemester Exam: 20% Endsem Exam: 20% Assignments : 50% Reading: 10%
Attendance requirements as per Institute norms	

Class	Coverage
[1] 16/1/2019 (W)	Introduction to the course
[2] 21/1/2019 (M)	**Packet Sniffing and Spoofing** Packet sniffing, BPF, Promiscuous mode
[3] 22/1/2019 (Tu)	BPF, eBPF, PCap
[4] 23/1/2019 (W)	PCap, Spoofing, UDP, ICMP, MAC spoofing
[5] 25/1/2019 (Fr)	Tutorial 1a: Packet Sniffing (TAs: Nikhilesh; Sourav Das)
[6] 28/1/2019 (M)	**TCP Attacks** TCP packets
[7] 29/1/2019 (Tu)	SYN flooding attacks, SYN cookies
[8] 30/1/2019 (W)	Ethical Hacking Talk (6:00PM)

[9] 1/2/2019 (Fr)	Tutorial 1b: Packet Spoofing (TAs: Nikhilesh; Sourav Das)
[10] 4/2/2019(M)	TCP connection closure
[11] 5/2/2019 (Tu)	Reset Attacks
[12] 6/2/2019 (W)	Session Hijacking Attack
[13] 8/2/2019 (Fr)	Tutorial 2a: TCP Attacks (TAs: Keerthi; Sourav Das)
[14]11/2/2019 (M)	**Firewalls** (stateless firewalls); netfilter
[15] 12/2/2019 (Tu)	iptables
[16] 13/2/2019 (W)	stateful firewalls; implementing issues in stateless firewalls; Firewall attacks
[17] 15/2/2019 (Fr)	Tutorial 2b: TCP Attacks (TAs: Keerthi; Sourav Das)
[18]18/2/2019 (M)	**DNS** introduction
[19] 19/2/2019 (Tu)	DNS Cache Poisoning Attacks
[20] 20/2/2019 (W)	DNS Remote Cache Poisoning Attacks
[21] 22/2/2019 (Fr)	Tutorial 3a: Firewalls (TAs: Gnanambikai, Sidharth)
[22] 25/2/2019 (M)	Distributed Denial of Service Attacks The Mirai Malware
[23] 26/2/2019 (Tu)	Bro Net filtering (Sareena K P)
[24] 27/2/2019 (W)	Detection and Mitigation of Mirai
[25] 1/3/2019 (Fr)	Tutorial 3b: Firewalls (TAs: Sareena, Gnanambikai, Sidharth)
[26] 4/3/2019 (M)	**Cryptography Primer** Cryptography: block ciphers and the AES
[27] 5/3/2019 (Tu)	Cryptography: AES implementation techniques
[28] 6/3/2019 (W)	Cryptography: hash functions
[29] 8/3/2019 (Fr)	Tutorial 4a: DNS Local Cache Poisoning (TAs: Himanshi, Sugandha)
[30] 11/3/2019 (M)	**Mid Semester Exam**

[31] 12/3/2019 (Tu)	Cryptography: MAC, public key ciphers;
[32] 13/3/2019 (W)	Cryptography: RSA
[33] 15/3/2019 (Fr)	Discussion session on the last tutorials
[34] 18/3/2019 (M)	Digital Signatures
[35] 19/3/2019 (Tu)	**Public Key Infrastructure** Certifying Authority, tree structure, x509 certificates
[36] 20/3/2019 (W)	building a PKI locally
[37] 22/3/2019 (Fr)	First CTF
[38] 25/3/2019 (M)	Attacks on PKI **Transport Layer Security**
[39] 26/3/2019 (Tu)	TLS client and server;
[40] 27/3/2019 (W)	TLS padding attack
[41] 28/3/2019 (Th)	Tutorial 5: PKI and TLS tutorial (TAs: Arsath and Jadhav)
[42] 1/4/2019 (M)	Poodle attack; BEAST; CRIME
[43] 2/4/2019 (Tu)	Heartbleed Attack
[44] 3/4/2019 (W)	**Key Establishment in IoT Environments**
[45] 5/4/2019 (Fr)	Tutorial 5 continued
[46] 8/4/2019 (M)	Blum's key establishment,
[47] 9/4/2019 (Tu)	key distribution; Fiat Noar key distribution
[48] 10/4/2019 (W)	Needham Schroeder Protocol for session key distribution
[49] 12/4/2019 (F)	Tutorial 6: Heartbleed attack (TAs: Gnanambikai, Sugandha)
[50] 16/4/2019 (Tu)	Kerberos and Bellare Rogaway session key distribution protocols
[51] 22/4/2019 (M)	**Virtual Private Networks**
[52] 23/4/2019 (Tu)	Setting up a TUN / VPN Client
[53] 24/4/2019 (W)	VPN / Security in IoTs (Prasanna Karthik)
[54] 1/5/2019	**Final Exam**