

Course name (English)	Advanced Network Security		
Course ID:	-	No of units:	3
Prerequisites:	Computer Networks		Program: Graduate
Co-requisites:			
Prepared by:	Mehdi Kharrazi		

Outline

- **Introduction to Network Security**
- **Threats and Attacks**
- **Firewalls**
- **IDS**
- **Denial of Service (DoS) attacks)**
- **Worms**
- **Botnets**
- **Honeypots**
- **Spyware**
- **Phishing Attacks**
- **Traffic Analysis**
- **Anonymity**
- **Routing Security**
- **Network Forensics**
- **Wireless Security**
- **VoIP Security**

References

1. Security Problems in the TCP/IP Protocol Suite, S.M. Bellovin, Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989.
2. An Introduction to Intrusion-Detection Systems, Hervé Debar, Proceedings of Connect'2000, Doha, Qatar, April 29th-May 1st, 2000.
3. Stalking the wily hacker, Cliff Stoll, Communications of the ACM 31:5, May 1988.
4. Exploiting P2P Systems for DDoS Attacks, N. Naoumov, and K.W. Ross, International Workshop on Peer-to-Peer Information Management, Hong Kong, May 2006.
5. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, Hari Balakrishnan, Transactions on Networking, Vol 11, 2003.
6. Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants), A. Kuzmanovic and E. Knightly, in Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003.
7. Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies, A. Kuzmanovic and E. Knightly, IEEE/ACM Transactions on Networking, 14(4):739-752, August 2006.
8. Automated Worm Fingerprinting, Sumeet Singh, Cristian Estan, George Varghese and Stefan Savage, Proceedings of the ACM/USENIX Symposium on Operating System Design and Implementation, San Francisco, CA, December 2004.
9. Fingerprinting by Random Polynomials, Michael O. Rabin. Center for Research in Computing Technology, Harvard University. Tech Report TR-CSE-03-01
10. Polygraph: Automatic Signature Generation for Polymorphic Worms James Newsome, Brad Karp, Dawn Song. In IEEE Security and Privacy Symposium, May 2005.
11. Anti-Honeypot Technology, Neal Krawetz of Hacker Factor Solutions, IEEE Security and Privacy, 2004.

12. Honeycomb — Creating Intrusion Detection Signatures Using Honeypots, C. Kreibich and J. Crowcroft. 2nd Workshop on Hot Topics in Networks (HotNets-II), 2003, Boston, USA.
13. Detecting Targeted Attacks Using Shadow Honeypots, K. G. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos, and A. D. Keromytis, 14th USENIX Security Symposium, 2005.
14. CANTINA: A Content-Based Approach to Detecting Phishing Web Sites, Yue Zhang, Jason Hong, Lorrie Cranor, WWW 2007.
15. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreantsason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, Proceedings of 14th ACM CCS, November 2007.
16. Low-resource routing attacks against tor, Kevin Bauer, Damon McCoy, Dirk Grunwald, Tadayoshi Kohno, Douglas Sicker, Workshop on Privacy in the Electronic Society, 2007.
17. Toward a Framework for Internet Forensic Analysis, V. Sekar, Y. Xie, D. Maltz, M. Reiter, H. Zhang, HotNets-III, 2004.
18. Payload Attribution via Hierarchical Bloom Filters, Kulesh Shanmugasundaram, Hervé Brönnimann, and Nasir Memon. ACM Computer Communications and Security (CCS 04), Washington, DC, 2004.
19. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting, J. Franklin, D. McCoy, P. Tabriz, V. Neagoie, J. Randwyk, D. Sicker, Usenix Security 2006.
20. A Survey of BGP Security, K. Butler, T. Farley, P. McDaniel, and J. Rexford, Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, Feb. 2004.