

Learning and teaching approaches:

Lecture, Demonstrations, Laboratory work, collaborative knowledge building, student research, student presentations, self-directed study

Required learning resources:

Michael Sikorski and Andrew Honig: *Practical Malware Analysis: A Hands-on Guide to Dissecting Malicious Software* (Paperback) No Starch Press, March 2012 ISBN: 9781593272906

After Semester 1 2014: selections from

Erez Metula: *Managed Code Rootkits: Hooking into Runtime Environments*
Syngress Media 2010 ISBN: 9781597495745

Recommended learning resources:

Michael Ligh, Steven Adair, Blake Hardstein and Matthew Richard: *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, John Wiley & Sons Ltd (2010) ISBN: 9780470613030

James M. Aquilina, Cameron H. Malin, Eoghan Casey and Rob Maxwell (Ed): *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides*, Syngress Media (2012) ISBN: 9781597494724

Jack Koziol, John Heasman, Felix Lindner, Gerardo Richarte, Dave Aitel, Chris Anley, Sinan Eren, Neel Mehta, Riley Hassell: *The Shellcoder's Handbook: Discovering and Exploiting Security Holes*, John Wiley & Sons Ltd (2007) ISBN: 9780470080238

Optional resources:

Adam Young and Moti Yung: *Malicious Cryptography: Exposing Cryptovirology*, John Wiley & Sons Ltd (2004) ISBN: 9780764549755