Course Description Network Security

Keywords: **Secure Protocols, Authentication, Identity Management, Firewalls, Intrusion Detection**

Audience:	**Semester AIM-IS1** **Semester AMI-IS2**	**Modul Number:**	**AIM 800 xxxx**
Workload:	**5 ECTS**		**150 h**
divided into	**Contact time**		**60 h**
	Self-study		**60 h**
	Exam preparation		**30 h**
Course language:	**English**		
Modul director:	**Prof. Dr. Tobias Heer**		
Vaild from:	**01.09.2020**		

Recommended requirements:

Understanding of computer networks, IT security and cryptography fundaments, basic programming skills

Desired learning outcomes of the module:

Students understand how to protect networks using both basic and advanced security methods.

Knowledge - professional competences

Students know:

- Network security objectives and basic attacks
- Security models for network protocols
- Cryptographic basics for network security protocols
- Security mechanisms on different network layers (e. g., PPP, IPsec, TLS, SSH)
- Authentication frameworks and identity management (e.g., OAuth, Kerberos, RADIUS)
- Basic protection solutions and devices (e.g., firewalls, VLAN, VPN, network monitoring, fail2ban)
- Advanced security mechanisms and algorithms (e.g., intrusion detection, honeypots)
- Anonymous communication

Skills - methodical competences

Students are able to

- Perform a security risk analysis for complex network deployments
- Select and implement network security methods
- Segment networks into security zones
- Design networks with regard to security
- Understand and use network security devices
- Understand anonymization techniques and their limitations

Comprehensive Competencies

Students be able to

- Deploy secure networked applications and IT services
- Leverage advanced concepts in network security

Contents:

- Network security goals, attacks and protection mechanisms
- Security mechanisms in the Internet (e.g., VLAN, IEEE 802.1X, IPsec, OpenVPN, TLS, SSH)
- Design and functions of network security protocols
- Authentication frameworks and identity management (e.g., Single-Sign-On, OAuth, Kerberos, PKI)
- Network attacks and counter-measures (e.g., firewalls, intrusion detection systems,)
- Advanced security solutions and research (e.g., intrusion detection, honeypots)
- Secure network operation and network monitoring

Literature:

- W. Stallings: Network Security Essentials, Pearson Prentice Hall, 2007
- N. Ferguson, B. Schneier: Practical Cryptography John Wiley & Sons, 2003
- G. Schäfer, M. Roßberg: Netzsicherheit, 2. Auflage, dpunkt Verlag, 2014
- C. Eckert: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg-Verlag, 2011
- R. Anderson: Security Engineering, Wiley, 2009
- B. Schneier: Applied Cryptography. Protocols, Algorithms, and Source Code in C. Wiley, New York 1996.

Offered:

Every summer semester

Submodules and Assessment:

Type of instruction:	Lecture with exercises and project work
Type of assessment:	Exam (90 minutes)
Hours per week:	4 SWS
Estimated student workload:	150 Hours

Generation of the module grade:

Exam

Modulbeschreibung Penetration Testing

Schlüsselwörter: IT-Sicherheit, Pentesting, Offensive Security

Zielgruppe:	**Semester AIM-IS1** **Semester AMI-IS2**	**Modulnummer:**	**800 xxxx**

Arbeitsaufwand:	**5 ECTS**	**150 h**
Davon	**Kontaktzeit**	**60 h**
	Selbststudium	**90 h**
	Prüfungsvorbereitung	**0 h**
Unterrichtssprache:	**Deutsch**	
Modulverantwortung	**Prof. Dr. Tobias Heer**	

Stand: **01.09.2020**

Empfohlene Voraussetzungen:

Kenntnisse über den Aufbau von Web-Applikationen und grundlegender Umgang mit den Betriebssystemen Windows und Linux.

Modulziel – angestrebte Lernergebnisse:
Um IT-Systeme auf Schwachstellen zu prüfen, ist ein Einblick in die Denkweise und Techniken von Angreifern unverzichtbar. Das Modul gibt einen Überblick über die offensive Seite der IT-Sicherheit und behandelt typische Schwachstellen und Angriffsmethoden.

Die Studierenden haben einen Überblick über die Vorgehensweise bei Angriffen auf IT-Systeme.
Sie wissen um die verfügbaren Tools und Methoden im Bereich der offensive Sicherheit.
Sie sind in der Lage, sicherheitsrelevante Informationen aus öffentlichen Quellen zu beschaffen (OSINT), verschiedene Schwachstellentypen in Web-Applikationen und Binäranwendungen zu erkennen, zu bewerten und auszunutzen sowie Gegenmaßnahmen vorzuschlagen.

Kenntnisse – fachliche Kompetenzen
Die Studierenden kennen
- offensive Sicherheitsmethoden und ihre Ziele im Kontext der IT-Sicherheit
- die wichtigsten Schwachstellen von IT-Systemen
- die Methodik von Penetrationstests
- gängige Risikofaktoren und Angriffsarten
- die rechtlichen und moralischen Rahmenbedingungen bei der Anwendung offensiver Sicherheitsmethoden

Fertigkeiten – methodische Kompetenzen
Die Studierenden sind in der Lage
- die wichtigsten Tools des Penetration Testing anzuwenden
- sich Zugang zu Systemen über Malware und offensive Sicherheitswerkzeuge zu verschaffen
- den Zugang zu übernommenen Systemen zu verstetigen
- relevante Informationen aus öffentlichen Quellen ermitteln und eine Analyse der Informationsfläche eines Ziels/Unternehmens durchzuführen
- Code auf Schwachstellen hin zu analysieren
- Schwachstellen zu entdecken und anhand von CVSS und anderen Metriken bewerten
- eine Sicherheitsüberprüfung durch einen Penetrationstest durchführen

Übergreifende Kompetenzen
Die Studierenden sind in der Lage
- Die IT-Sicherheit von IT-Systemen zu prüfen und zu bewerten.

Inhalt:

- Methodik und Ablauf eines Penetrationstests
- Rechtliche Stoplerstricke und Rechtslage

- Angriffsfläche und des Informations-Footprint eines Unternehmens
- Erkennen und Bewerten typischer Schwachstellen in IT-Systemen
- Angriffstypen, Angriffsvektoren und Windows und Linux Systemen
- Malware-Verschleierung und Angriffswerkzeuge
- Persistenten Zugang über verschiedene Methoden erreichen
- Praktische Durchführung von Angriffen

Literaturhinweise:

- Kim, P.: The Hacker Playbook 2, A practical Guide to Penetration Testing, Secure Planet LLC, 2015
- Hadnagy, C.: Social Engineering, The Art of Human Hacking, Wiley Publishing Inc., 2011
- Stuttard D.: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Auflage 2, John Wiley & Sons, 2011
- Erickson, J.: Hacking, The Art of Exploitation, No Starch Press, 2008
- Messner, M.: Metasploit: Das Handbuch zum Penetration-Testing-Framework, dpunkt.Verlag, 2015

Wird angeboten:

In jedem Wintersemester

Teilgebiete und Leistungsnachweise:

Lehr-, Lernform:	Vorlesung und Projektarbeit
Leistungskontrolle:	Bericht und Fortschritt bei den praktischen Übungen
Anteil Semesterwochenstunden:	4 SWS (3 SWS Vorlesung, 1 SWS Projektbetreuung)
Geschätzte studentische Arbeitszeit:	150 Stunden

Bildung der Note:

benoteter Bericht und Abschlusspräsentation