# MACS H6011: Network Security

| | |
|---|---|
| **Short Title:** | Network Security APPROVED |
| **Full Title:** | Network Security |

| | |
|---|---|
| **Module Code:** | MACS H6011 |

| | |
|---|---|
| **ECTS credits:** | 10 |

| | |
|---|---|
| **NFQ Level:** | 9 |

| | |
|---|---|
| **Module Delivered in** | 3 programme(s) |

| | |
|---|---|
| **Module Contributor:** | Mark Lane |

| | |
|---|---|
| **Module Description:** | Module content includes: • Investigation of core security technologies and security policies to mitigate risks. • Ability to review procedures for installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices. • Knowledge of the technologies that underpin the deployment and maintenance of a secure network. |

**Learning Outcomes:**

*On successful completion of this module the learner will be able to*

1. Appraise the underlying theories of networking communication protocols and application protocols.
2. Investigate and appraise popular Intrusion Detection and Prevention Systems.
3. Expertly utilise traffic analysis tools to critically analyse network traffic and identify signs of an intrusion

## Module Content & Assessment

| Indicative Content |
|---|
| **Fundamentals of Traffic Analysis**<br>Concepts of TCP/IP, TCP/IP communications model, Data encapsulation/de-encapsulation, bits, bytes, binary, and hex Introduction to Wireshark, Navigating Wireshark, statistics, Stream reassembly, Finding content in packets Network Access/Link Layer: Layer 2, 802.x link layer, Address resolution protocol, ARP spoofing IP Layer: Layer 3, IPv4 fields, Checksums, Fragmentation: IP header fields involved in fragmentation, composition of the fragments, fragmentation attacks IPv6: Comparison with IPv4, IPv6 addresses, Neighbour discovery protocol, Extension headers |
| **Traffic Analysis in Practice**<br>Wireshark Display Filters: creating display filters, Composition of display filters Writing tcpdump Filters, Format of tcpdump filters TCP: TCP fields, Packet dissection, Checksums, Normal and abnormal TCP activity, Importance of TCP reassembly for IDS/IPS UDP: Examination of fields in theory and practice, UDP activity ICMP: Use of ICMP, mapping and reconnaissance, Normal ICMP, Malicious ICMP |
| **Application Protocols**<br>Detection Methods for Application Protocols: Pattern matching, protocol decode, and anomaly detection, Detection challenges Protocols: SMB/CIFS, MSRPC, HTTP (format, attacks), SMTP, DNS )role, resolution, caching, DNSSEC, malicious DNS, cache poisoning |
| **Open-Source IDS**<br>Open-Source IDS: Planning, installation, configuration, running, auditing and updating, Function of an IDS: analyst role, flow process, Snort, Bro Snort: Introduction, planning and deployment, modes, plug-ins, writing rules, refining, sniffer, packet logger, NIDS Introduction to Bro: Planning, Operational modes (Standalone/cluster), Running (BroControl), policy neutral features, scripting, Signatures Comparing Snort and Bro |
| **IDS/IPS Evasion**<br>IDS/IPS Evasion: evasions at different protocol layers, target-based detection Real-World Traffic Analysis: Client attacks, DDoS attacks, Four-way handshake, TCP reset attack, Malformed DNS DoS |

| Indicative Assessment Breakdown | % |
|---|---|
| Course Work Assessment % | 100.00% |

**Course Work Assessment %**

| *Assessment Type* | *Assessment Description* | *Outcome addressed* | *% of total* | *Assessment Date* |
|---|---|---|---|---|
| Case study | Group project | 1,2 | 30.00 | Week 5 |
| Practical/Skills Evaluation | Research Paper | 2 | 35.00 | Week 8 |
| Written Report | Written report and lab demonstration/presentation | 2,3 | 35.00 | Sem 1 End |

No Final Exam Assessment %

| Indicative Reassessment Requirement |
|---|
| **Coursework Only**<br>*This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.* |
| **Reassessment Description**<br>Reassessment is individual and based on a major research project. Deliverables include a research paper, lab demonstration and presentation. |

**ITB reserves the right to alter the nature and timings of assessment**

## Indicative Module Workload & Resources

| Indicative Workload: Full Time | |
|---|---|
| **Frequency** | **Indicative Average Weekly Learner Workload** |
| Every Week | 2.00 |
| Every Week | 2.00 |
| Every Week | 6.00 |

| Indicative Workload: Part Time | |
|---|---|
| **Frequency** | **Indicative Average Weekly Learner Workload** |
| Every Week | 2.00 |
| Every Week | 2.00 |
| Every Week | 6.00 |

**Resources**

*Recommended Book Resources*

**by Richard Bejtlich.,** ***The practice of network security monitoring*****, San Francisco; No Starch Press [ISBN: 1593275099]**

**Laura Chappell, Gerald Combs (Foreword),** ***Wireshark Network Analysis (Second Edition)*****, Laura Chappell University [ISBN: 1893939444]**

*Recommended Article/Paper Resources*

**SANS** ***SANS Reading Room***
https://www.sans.org/reading-room/

**Elsevier** ***Network Security Journal***
http://www.journals.elsevier.com/network-security/

*Other Resources*

**Internet based resource: Bruce Schneier*****Schneier on Security***
https://www.schneier.com

**Internet based resource: OWASP*****Open Web Application Security Project***
https://www.owasp.org

**Internet based resource: Sourcefire*****Snort IDS***
https://snort.org/

**Internet based resource: *****Top 10 Network Security Tools***
http://sectools.org/

## Module Delivered in

| Programme Code | Programme | Semester | Delivery |
|---|---|---|---|
| BN_EMIOT_R | Master of Engineering in Internet of Things Technologies [BN535R 60 credits taught with a 30 credit research project] | 2 | Elective |
| BN_KMACS_R | Master of Science in Computing in Applied Cyber Security | 1 | Mandatory |
| BN_KMACS_M | Master of Science in Computing in Applied Cyber Security (Research) | 1 | Group Elective 1 |