Note: This schedule is tentative and may change later.

Different units in the course are indicated by different colors.

Unit	Week	Date	Topic	Lecturer	Readings	Slide
Introduction	1	Sep 4	Introduction	Instructor	The security mindset (web) Advanced Persistent Threat Explained (web) What is Cyber Threat Intelligence? (web) How to Read a Paper. S. Keshav (pdf)	Course Intro Handout_1
Authentication	2	Sep 9	Authentication and identity	Instructor		Handout_2
Threats and defenses	2	Sep 11	Auditing/logging	Instructor		Handout_3
	3	Sep 16	Intrusion Detection Systems	Instructor		Handout_4
	3	Sep 18		Instructor	PERMON: An OpenStack Middleware for Runtime Security Policy Enforcement in Clouds, SPC'18 (pdf) Assignment 1 Introduction: prepare a presentation on the CVE exploits, the demo on the exploit execution, showing the sysdig/AuditD relevant logs (detailed instructions and grade breakdown will be on UM Learn)	
Provenance Audit logging	4	Sep 23	Audit logging with data provenance	Instructor	https://github.com/ashish-gehani/SPADE/wiki	To be uploaded
	4	Sep 25		Instructor	Backtracking Intrusions (pdf) Assignment 2 Introduction: prepare a video+presentation showing that could enable SPADE, collect provenance in Linux, view provenance, show relevant attack steps for the same exploit as in Assignment 1 (detailed instructions and grade breakdown will be on UM Learn)	To be uploaded
	5	Sep 30				
Investigation	5	Oct 2		Devon	Back-Propagating System Dependency Impact for Attack Investigation (pdf) **Project discussion**: to get more relevant and in-time feedback, students are required to prepare a few slides on their proposal Assignment1 presentation	To be uploaded
	6	Oct 7		All	~~**Assignment 2 presentations** (spade)~~ Assignment1 presentation (cont') **Useful resources** for better understanding of next units: - But what is a neural network? | Chapter 1, Deep learning (video) - But what is a GPT? Visual intro to transformers | Chapter 5, Deep Learning (video)	To be uploaded
	6	Oct 9		Instructor	ATLAS: A Sequence-based Learning Approach for Attack Investigation, USENIX Security' 21 (pdf)	To be uploaded
	~~7~~	~~Oct 14~~		~~Md Nahidul~~	~~Tactical Provenance Analysis for Endpoint Detection and Response Systems~~ **Proposal presentation:** students are required to prepare and submit a few slides on their proposal (note the steps you have done so far, and anticipated challenges ahead (details on UM Learn)	
Threat Hunting	7	Oct 16		Md Nahidul	Tactical Provenance Analysis for Endpoint Detection and Response Systems	
				Jack	Deephunter: A graph neural network based approach for robust cyber threat hunting (pdf) Assignment3 Introduction: prepare a survey for a thorough comparison on papers in Threat Hunting and Investigation units (detailed instructions and grade break down will be on UM Learn).	
	8	Oct 21		Eddie	ProvG-Searcher: A Graph Representation Learning Approach for Efficient Provenance Graph Search (pdf) **Assignment2 in-class presentations** (each assignment should be strictly 10 min max)	**Please check submission deadline for Assignment 2 and 3**

Provenance-based Intrusion Detection	8	Oct 23	Temporal evolution	Md Shahidul	**Assignment3 in-class presentations** (each assignment should be strictly 10 min max) UNICORN: Runtime Provenance-Based Detector for Advanced Persistent Threats, NDSS'20 (pdf)	
	9	Oct 28		Fairuz	KAIROS: Practical Intrusion Detection and Investigation using Whole-system Provenance (pdf) Auxiliary resource (useful to better understand FLASH): Attention in transformers, visually explained | Chapter 6, Deep Learning (video)	
	9	Oct 30		Baha	FLASH: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning, IEEE S&P'24 (pdf) Assignment 4 Introduction: prepare a survey for a thorough comparison on papers in provenance-based intrusion detection unit (detailed instructions and grade break down will be on UM Learn).	
	10	Nov 4	Different granularities	Magdy Cenker	MAGIC: Detecting Advanced Persistent Threats via Masked Graph Representation Learning, USENIX'24 (pdf) NODLINK: An Online System for Fine-Grained APT Attack Detection and Investigation, NDSS'244 (pdf)	
	10	Nov 6			**Assignment 4 presentations**	
	11	Nov 11		N/A		
	11	Nov 13		N/A		
	12	Nov 18		all	**Project Progress presentation**	
What is overlooked?	12	Nov 20		Instructor Aden	Mimicry Attacks on Host-Based Intrusion Detection Systems, CCS'2 (pdf) Evading Provenance-Based ML Detectors with Adversarial System Actions, USENIX'23 (pdf)	
Provenance in other systems	13	Nov 25	Management-level provenance for virtualized environments	Instructor	Catching Falling Dominoes: Cloud Management-Level Provenance Analysis with Application to OpenStack, CNS 2020 (pdf) ProvTalk: Towards Interpretable Multi-level Provenance Analysis in Networking Functions Virtualization (NFV), NDSS'22 (pdf)	
Network security	13	Nov 27		Instructor	Signaling Storm	
Deliverables and exam	14	Dec 4			Final exam **(Presentation video due Dec 9 by midnight)**	
	14	Dec 9			Project Presentation	
					The remaining course project deliverables (e.g., code comments, report, etc.) are due Dec 9 as well.	