Secure Systems Engineering
Jan - May 2025

Schedule

Sl	Date	Topic
01	2025-01-16 (M)	Introduction to the course
02	2025-01-17 (Tu)	**Binary Exploitation** Exploit and Vulnerabilities; Buffer overflows on the stack. Stack exploit, injecting code into stack to create a shell
03	2025-01-19 (Th)	**Tutorial:**Demonstration of gdb, objdump, stack configuration
03	2025-01-27 (M)	Canaries and W^X
04	2025-01-28 (Tu)	ROP attacks
05	2025-01-30 (Th)	**Assignment 1:** buffer overflows
06	2025-02-04 (Tu)	More on ROP attacks,
08	2025-02-06 (Th)	ASLR. Load time relocation
09	2025-02-10 (M)	Position Independent Code; PLT Tables for functions, etc
10	2025-02-11 (Tu)	More on ASLR, Fatpointers, SoftBound, etc. Buffer overread
11	2025-02-13 (Th)	Quiz 1: Syllabus till 2025-02-10. **Assignment 2**
12	2025-02-17 (M)	Buffer overread and Heardbleed; Format String Vulnerabilities
13	2025-02-18 (Tu)	Format String Vulnerabilities; Integer overflow vulnerabilities
14	2025-02-20 (Th)	Quiz 1 answer scripts
15	2025-02-24 (M)	Integer overflow vulnerabilities; Heap exploits
16	2025-02-25 (Tu)	Heap Exploits
17	2025-02-27 (Th)	**Assignment 3: ROPs**
18	2025-03-03 (Tu)	**Malware. Types of Malware.** Mirai.
19	2025-03-05 (Th)	Advanced Persistent Threats
20	2025-03-10 (M)	Stuxnet APT internals
21	2025-03-11 (Tu)	Demonstration of firmware extraction and reverse

		engineering (Ritwik Badola) **Assignment 4:** Reverse Engineering a router
22	2025-03-13 (M)	Malware evasion and polymorphic and metamorphic malware.
23	2025-03-14 (Tu)	Dynamic malware evasion and D-TIME
24	2025-03-17 (M)	**Access Control.** Discretionary Access Control (DAC)
25	2025-03-18 (Tu)	Unix access control policies
26	2025-03-24 (M)	**Quiz 2:** Syllabus till Unix access control policies (class 25)
27	2025-03-27 (Th)	MAC and Bell-Lapadula Model
28	2025-04-01 (Tu)	**Principle of Least Privileges.** **OKWS Web Server Design**
29	2025-04-07 (M)	OKWS; NACL Software fault Isolation
30	2025-04-08 (Tu)	SFI: Software Fault Isolation
31	2025-04-15 (Tu)	**Trusted Execution Environments**
32	2025-04-21 (M)	Securing a UPI application with ARM trustzone.
33	2025-04-24 (Th)	Secure boot and secure update
34	2025-04-28 (M)	Intel's SGX