**CIFR Class Schedule**

|  |  |  |
| --- | --- | --- |
| Day | Week 1 | Week 2 |
| Monday | Lecture:* Network theory
* Microsoft network architecture

Labs:* Remote Desktop
* Join an AD domain
* Use of net.exe commands
* Create group policies (GPOs)
 | Lecture:* Windows event logs
* Windows image analysis focusing on malware and intrusion artifacts

Labs:* Event log analysis with Event Log Explorer
* Event log analysis with Log Parser and Log Parser Studio
* Windows artifacts extraction and analysis
 |
| Tuesday | Lecture:* Log types, locations and contents
* Wireshark

Labs:* Use of Wireshark
* Wireshark scenario
 | Lecture:* Linux fundamentals
* Linux analysis

Labs:* Analysis of compromised Linux image
 |
| Wednesday | Lecture:* Linux commands for log analysis

Labs:* Use Linux commands for log analysis of multiple log types
 | Lecture:* RAM capture and analysis

Labs:* RAM capture with multiple tools
* RAM analysis with Volatility 3 and other tools
 |
| Thursday | Lecture:* Remote analysis
* Remote imaging
* Use of Velociraptor for analysis at scale

Labs:* Capture Windows image across the network using FTK Image CLI and netcat
* Capture Linux image across the network using dd and netcat
* Capture Linux image across the network using dd and ssh
* Remote analysis with Forensic Explorer
* Remote analysis with Velociraptor
 | Lecture:* Static and dynamic malware analysis

Labs:* Static and dynamic malware analysis of Office documents, PDFs, and Windows executables

Capstone Exercise:* Walkthrough of PowerShell Empire
* Walkthrough of mimikatz
* Walkthrough of scripted deployment of ransomware
* Capture RAM across the network
* Capture drive image across the network
 |
| Friday | Lecture:* Log2Timeline / Plaso

Labs:* Log2Timeline / Plaso timeline generation and analysis
* ssh attack log analysis
* Web server attack log analysis
 | Lecture:* Guided analysis processes for capstone evidence

Labs:* Analyze capstone evidence
 |