

## Net Sec Lab

Class 1: Lecture - Linux Skills and Firewalls - Douglas Sicker

Class 2: Lecture and Guided Lab

Class 3: Independent Lab

Class 4: Lecture - Intrusion Detection & SNORT

Class 5: Lab - SNORT/ACID setup

Class 6: Lab - SNORT use, analysis of normal network use, reporting, etc

Class 7: Lecture - Vulnerability Assessment/Scanning & Nmap - Nessus (discussion points include differences in approaches with and without a firewall)

Class 8: Lab - Setup and use of Nessus and Nmap (discussion points include differences in approaches with and without a firewall)

Class 9: Lab - Vulnerability Scanning with Nessus and Nmap and how this shows on SNORT IDS Console

Class 10: Lecture - System Hardening

Class 11: Lab - Nessus and Nmap use against hardened system, semi-hardened system, non-hardened system

Class 12: Lab - Reconciling SNORT reports of Nessus and Nmap scans against all three levels of hardened systems

- \* Discussion point - SNORT reports to all three systems look the same, which system was truly vulnerable?

- \* Research point - Verifying which systems are truly vulnerable and which were hardened

Class 13: Lecture - Forensic Tools Primer (incl. Encase) & Brief Methodology Review (option)

Class 14: Lab - Investigating the victim systems

Class 15: Lab - Investigating the victim systems & Reporting

Class 16: How were the victim systems compromised?