

| <b>DAY 1 Incident Response</b>                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Module 1: Introduction to Incident Response                                                                                                                                                                                                                                                                                                                                                                                    |
| Understanding the different phases in incident response                                                                                                                                                                                                                                                                                                                                                                        |
| Plan                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Identify                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Contain                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Eradicate                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Recover                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>LAB(PRACTICAL)</b>                                                                                                                                                                                                                                                                                                                                                                                                          |
| • Event/incident detection – using splunk (SIEM)                                                                                                                                                                                                                                                                                                                                                                               |
| • Sources of network evidence – using wireshark tool                                                                                                                                                                                                                                                                                                                                                                           |
| • NIDS/NIPS – using snort                                                                                                                                                                                                                                                                                                                                                                                                      |
| Incident Response and Cyber Investigations                                                                                                                                                                                                                                                                                                                                                                                     |
| MITRE ATT&CK Framework                                                                                                                                                                                                                                                                                                                                                                                                         |
| cyber kill chain methodology                                                                                                                                                                                                                                                                                                                                                                                                   |
| Tactics, Techniques, and Procedures (TTPs)                                                                                                                                                                                                                                                                                                                                                                                     |
| Adversary Behavioral Identification                                                                                                                                                                                                                                                                                                                                                                                            |
| Indicators of Compromise (IoCs)                                                                                                                                                                                                                                                                                                                                                                                                |
| Diamond Model of Intrusion Analysis                                                                                                                                                                                                                                                                                                                                                                                            |
| Module 4: Real life scenarios on cyber-Incidents and remediation                                                                                                                                                                                                                                                                                                                                                               |
| • Privilege abuse                                                                                                                                                                                                                                                                                                                                                                                                              |
| • Insider data theft                                                                                                                                                                                                                                                                                                                                                                                                           |
| • Intellectual property theft                                                                                                                                                                                                                                                                                                                                                                                                  |
| • Third-party vendor attacks                                                                                                                                                                                                                                                                                                                                                                                                   |
| • Internet-Facing vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                              |
| • Business Email Account takeover                                                                                                                                                                                                                                                                                                                                                                                              |
| • Incident response playbooks                                                                                                                                                                                                                                                                                                                                                                                                  |
| • DOS attack                                                                                                                                                                                                                                                                                                                                                                                                                   |
| LAB(PRACTICAL)                                                                                                                                                                                                                                                                                                                                                                                                                 |
| • Phishing attack                                                                                                                                                                                                                                                                                                                                                                                                              |
| • Ransomware                                                                                                                                                                                                                                                                                                                                                                                                                   |
| • Malware                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>DAY 2 Incident response continued and Forensics</b>                                                                                                                                                                                                                                                                                                                                                                         |
| Overview                                                                                                                                                                                                                                                                                                                                                                                                                       |
| In this course section we'll begin our look at target exploitation frameworks that take advantage of weaknesses on public servers and client-side vulnerabilities. Using the implicit trust of a public website, you'll apply attacker tools and techniques to exploit browser vulnerabilities, execute code with Microsoft Office documents, and exploit the many vulnerabilities associated with vulnerable web applications |
| Exercises                                                                                                                                                                                                                                                                                                                                                                                                                      |
| • SQL injection                                                                                                                                                                                                                                                                                                                                                                                                                |
| ◦ Command Injection Attack                                                                                                                                                                                                                                                                                                                                                                                                     |
| ◦ Cross-Site Scripting Attack                                                                                                                                                                                                                                                                                                                                                                                                  |
| ◦ Web application vulnerability scanning by Nikto, Nessus                                                                                                                                                                                                                                                                                                                                                                      |
| ◦ Web application security                                                                                                                                                                                                                                                                                                                                                                                                     |
| ◦ OWASP top 10 vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                                 |
| Incident response and recovery                                                                                                                                                                                                                                                                                                                                                                                                 |
| ◦ Live Windows examination – using Dumpit, ftk imager, acquiring volatile data using cmd                                                                                                                                                                                                                                                                                                                                       |
| ◦ Network investigation- using wireshark and splunk                                                                                                                                                                                                                                                                                                                                                                            |

|                                                                                    |
|------------------------------------------------------------------------------------|
| ◦ Memory investigation – using volatility and redline                              |
| ◦ Malware investigation – using static and dynamic tools                           |
| <b>Day 3: Forensics</b>                                                            |
| NETWORK INVESTIGATIONS                                                             |
| • Network and Host Scanning with Nmap                                              |
| • Host enumeration and discovery with Nmap                                         |
| • Internal and external network mapping and visualization                          |
| • Minimizing network activity to avoid detection                                   |
| • Deep host assessment with Nmap Scripting Engine tool                             |
| • Website Reconnaissance                                                           |
| • Information-gathering from public websites                                       |
| • Parsing Exchangeable Image File Format (EXIF) data from public documents         |
| • Optimizing search engine reconnaissance interrogation                            |
| • Abstracting attack identification using public sources                           |
| Command Injection attack - metasploitable                                          |
| OS Credential Dumping - mimikatz                                                   |
| Windows and Linux OS In-Depth Architecture                                         |
| Collecting Volatile Information in a Windows System                                |
| Framework and Lifecycle of Digital Forensics                                       |
| Chain of Custody Procedures and Practices                                          |
| Importance of Forensic Acquisition with Write-Blocker                              |
| Viewing, Monitoring, and Analyzing Events in a Windows System                      |
| Hands-On Analysis with FTK and Autopsy                                             |
| Lesson Learned Documentation and Practice                                          |
| Q&A Session and Wrap-up                                                            |
| <b>Day 4: Threat Hunting</b>                                                       |
| Recap of Previous Day                                                              |
| Diamond Model and Threat Modeling                                                  |
| Open-Source Intelligence Collection Tools and Frameworks – osint,recon-            |
| ng,maltego,shodan,theHarvester                                                     |
| MITRE attack framework                                                             |
| Triage Analysis and Timeline Analysis with ELK                                     |
| Files-less Malware Analysis and Firewall, Switch, and Router Log Analysis          |
| Applying Visualizer for Analysis and Mining Application Logs for Suspicious Events |
| Q&A Session, Final Remarks, and Training Conclusion                                |