Blue Team Penetration Testing Hands On Workshop

Duration : 5 Days

- Identify type of attacks
- Identify intrusions on the systems
- Identify and block the attacks before they succeed
- Activate run books for incident response
- Stay alert for reactive or preventive action
- Train the physical security teams for identity spoof
- Enhance security standards
- Activate the containment of attacked systems
- Logs and SIEM Config/Alerts
- Security awareness training
- Check on domain expirations
- Email filters, threshold, and spam rules
- Two-factor authentication
- Deny long relay request
- Application whitelisting
- Segmentation
- Manage keys securely
- Config and patch management
- Secure group policy settings
- Sensitive data stores