ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

Blue Team Level 1

Course Syllabus

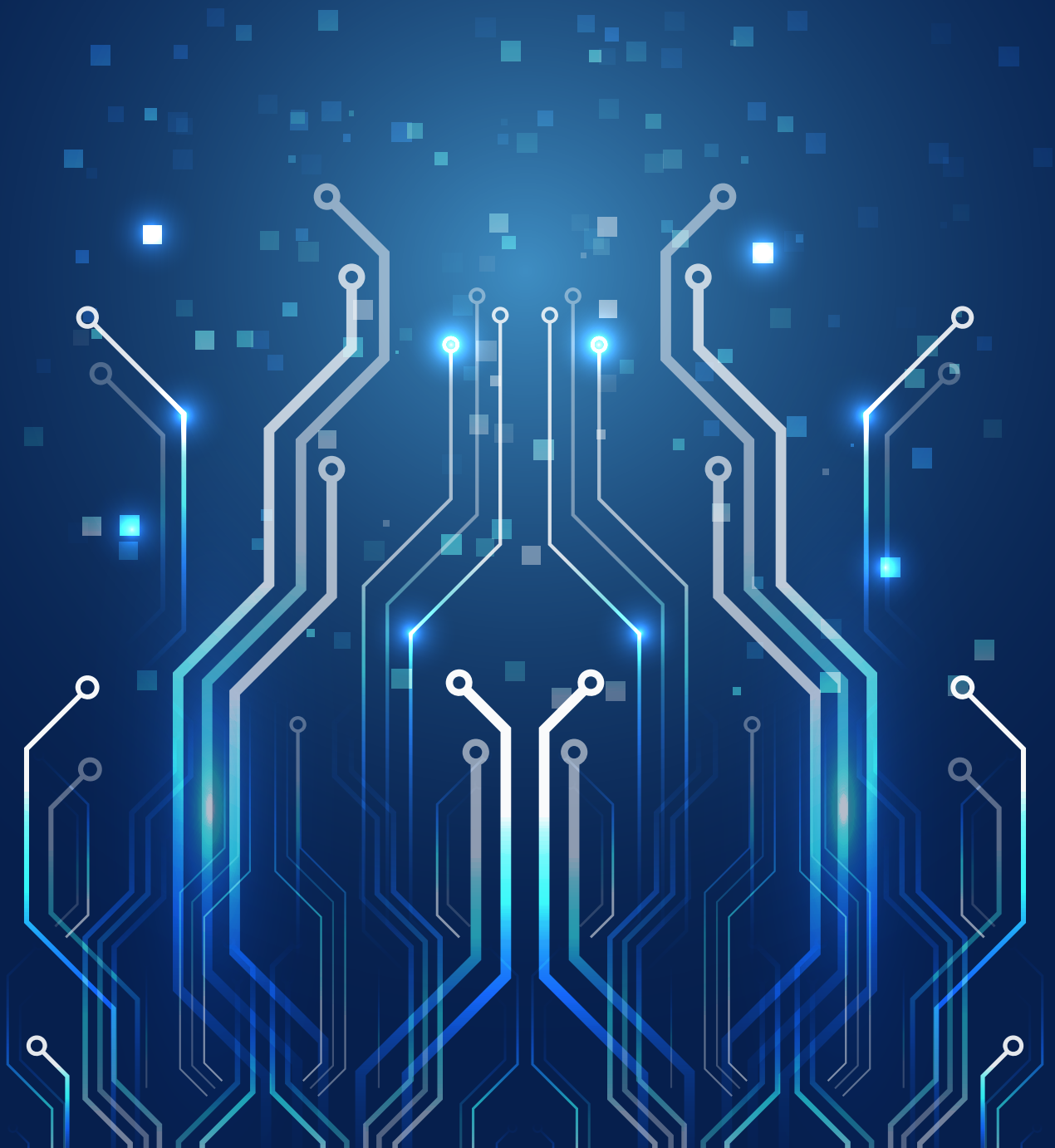

Table of Contents

ABAD NETWORK FOR TRAINING

Introduction

Why did we make BTL1?

At the time of release (June 2020) there was a huge imbalance of training content, heavily favouring red team (offensive) over blue team (defensive). We wanted to create a modern, practical, and realistic blue team certification to advance the skills of aspiring or established defenders around the world.

Copyright Notice

Access Terms and Conditions

During the checkout process students must agree to the Refunds Policy and BTL1 Terms and Conditions before they are able to purchase the course. These terms are also reiterated at the start of the course. These protect the intellectual property of Security Team Training Ltd and prohibit students from sharing training material with non-students. Any form of piracy, account sharing, or otherwise disclosing private course materials will result in permanent account termination with no refund, and potentially legal action to claim for damages. Please respect our hard work.

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

Domain 1: Security Fundamentals

Introduction

- Introduction to Security Fundamentals
- Blue Team Roles

Soft Skills

- Section Introduction, Soft Skills
- Communication
- Teamwork
- Problem Solving
- Time Management
- Motivation
- Mental Health

Security Controls

- Section Introduction, Security Controls
- Physical Security
- Network Security
- Endpoint Security
- Email Security
- Activity) End of Section Review

Networking 101

- Section Introduction, Networking 101
- Network Fundamentals
- The OSI Model
- Network Devices
- Network Tools
- Ports and Services
- Activity) Conducting a Port Scan With Nmap
- Activity) End of Section Review

Management Principles

- Section Introduction, Management Principles
- Risk
- Policies and Procedures
- Compliance & Frameworks

ABAD
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

Domain 2: Phishing Analysis (1/2)

PA1) Introduction

- Section Introduction, Emails and Phishing
- How Electronic Mail Works
- Anatomy of an Email
- What is Phishing?
- Impact of Phishing
- Further Reading Material
- Phishing Analysis Glossary
- Activity) End of Section Review

PA2) Types of Phishing Emails

- Section Introduction, Phishing Emails
- Reconnaissance
- Spam
- False Positives
- Credential Harvester
- Social Engineering
- Vishing and Smishing
- Whaling
- Malicious Files
- Video) Types of Phishing Attacks
- Activity) Categorising Phishing Emails
- Activity) End of Section Review

PA3) Tactics and Techniques

- Section Introduction, Tactics and Techniques
- Spear Phishing
- Impersonation
- Typosquatting and Homographs
- Sender Spoofing
- HTML Styling
- Attachments
- Hyperlinks
- URL Shortening
- Use of Legitimate Services
- Business Email Compromise
- Video) Tactics and Techniques
- Activity) Reporting on Tactics Used
- Activity) End of Section Review

PA4) Investigating Emails

- Section Introduction, Investigating Emails
- Artifacts we Need to Collect
- Manual Collection - Email Artifacts
- Manual Collection - Web Artifacts
- Manual Collection - File Artifacts
- Video) Collecting Artifacts - Manual
- Automated Collection With PhishTool
- Video) Collecting Artifacts - Automated
- Activity) Manual Artifact Extraction
- Activity) End of Section Review

Domain 2: Phishing Analysis (2/2)

PA5) Analyzing Artifacts

- Section Introduction, Analyzing Artifacts
- Visualization Tools
- URL Reputation Tools
- File Reputation Tools
- Malware Sandboxing
- Video) Manual Artifact Analysis
- Artifact Analysis with PhishTool
- Video) Artifact Analysis with PhishTool
- Activity) End of Section Review

PA6) Taking Defensive Actions

- Section Introduction, Defensive Measures
- Preventative: Marking External Emails
- Preventative: Email Security Technology
- Preventative: Spam Filter
- Preventative: Attachment Filtering
- Preventative: Attachment Sandboxing
- Preventative: Security Awareness Training
- Reactive: Immediate Response Process
- Reactive: Blocking Email Artifacts
- Reactive: Blocking Web Artifacts
- Reactive: Blocking File Artifacts
- Reactive: Informing Threat Intelligence
- Activity) End of Section Review

PA7) Report Writing

- Section Introduction, Report Writing
- Email Header, Artifacts, Body Content
- Analysis Process, Tools, Results
- Defensive Measures Taken
- Activity) Report Writing
- Activity) Report Writing Contd.
- Activity) End of Section Review

PA8) Lessons Learned

- Section Introduction, Lessons Learned
- Identifying New Tactics
- Response Improvements

PA9) Phishing Challenge

- Section Introduction, Phishing Response
- Video) Phishing Response Walkthrough
- Phishing Response Brief
- Activity) Phishing Response

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

Domain 3: Threat Intelligence (1/2)

TI1) Introduction

- Section Introduction, Threat Intelligence
- Threat Intelligence Explained
- Why Threat Intelligence can be Valuable
- Types of intelligence
- The Future of Threat Intelligence
- Further Reading
- Threat Intelligence Glossary

TI2) Threat Actors and APTs

- Section Introduction, Actors
- Common Threat Agents
- Motivations
- Actor Naming Conventions
- What are APTs?
- Tools, Techniques, Procedures
- Activity) Threat Actor Research
- Activity) End of Section Review

TI3) Operational Intelligence

- Section Introduction, Operational Intelligence
- Precursors Explained
- Indicators of Compromise Explained
- MITRE ATT&CK Framework
- Lockheed Martin Cyber Kill Chain
- Attribution and its Limitations
- Pyramid of Pain
- Activity) End of Section Review

TI4) Tactical Intelligence

- Section Introduction, Tactical Intelligence
- Threat Exposure Checks Explained
- Watchlists/IOC Monitoring
- Public Exposure Checks Explained
- Threat Intelligence Platforms
- Malware Information Sharing Platform
- Activity) Deploying MISP
- Activity) End of Section Review

Domain 3: Threat Intelligence (2/2)

TI5) Strategic Intelligence

- Section Introduction, Strategic Intelligence
- Intelligence Sharing and Partnerships
- IOC/TTP Gathering and Distribution
- OSINT vs Paid-For Sources
- Traffic Light Protocol (TLP)
- Activity) End of Section Review

TI6) Global Malware Campaigns

- Section Introduction, Global Campaigns
- Malware Used by Threat Actors
- Global Campaign: Trickbot
- Global Campaign: Sodinokibi
- Global Campaign: Magecart
- Global Campaign: Emotet
- Activity) End of Section Review

Domain 4: Digital Forensics (1/2)

DF1) Introduction

- Section Introduction, Digital Forensics
- What is Digital Forensics?
- Digital Forensics Process
- Further Reading
- Threat Intelligence Glossary
- Activity Download List

DF2) Forensics Fundamentals

- Section Introduction, Forensics Fundamentals
- Introduction to Data Representation
- Activity) Data Representation
- Hard Disk Drive Basics
- SSD Drive Basics
- File Systems
- Activity) File Systems
- Digital Evidence and Handling
- Order of Volatility
- Metadata and File Carving
- Activity) Metadata and File Carving
- Memory, Pagefile and Hibernation File
- Hashing and Integrity
- Activity) Hashing and Integrity
- Activity) End of Section Review

DF3) Digital Evidence

- Section Introduction, Evidence Collection
- Equipment
- ACPO Principles of Evidence and Preservation
- Chain of Custody
- Disk Imaging: FTK Imager
- Live Forensics
- Live Acquisition: KAPE
- Evidence Destruction
- Activity) End of Section Review

DF4) Windows Forensics

- Section Introduction, Windows Investigations
- Windows Artifacts - Programs
- Activity) Windows Investigation 1
- Windows Artifacts - Browsers
- Activity) Windows Investigation 2
- Activity) End of Section Review

Domain 4: Digital Forensics (2/2)

DF5) Linux Forensics

- Section Introduction, Linux Investigations
- Linux Artifacts - Shadow and Passwd
- Activity) Password Cracking
- Linux Artifacts - /Var/Lib and /Var/Log
- Linux Artifacts - User Files
- Activity) End of Section Review

DF6) Volatility

- Section Introduction, Volatility
- What is Volatility?
- Volatility Walkthrough
- Activity) Volatility Exercise

DF7) Autopsy

- Section Introduction, Autopsy
- What is Autopsy?
- Installing Autopsy
- Autopsy Walkthrough
- Activity) Autopsy Exercise

Domain 5: Security Information and Event Management

SI1) Introduction

- Section Introduction, SIEM
- Security Information Management (SIM)
- Security Event Management (SEM)
- What is a SIEM?
- SIEM Platforms
- Further Reading
- SIEM Glossary
- Activity) End of Section Review

SI2) Logging

- Section Introduction, Logging
- What is Logging?
- Syslog
- Windows Event Logs
- Sysmon
- Other Logs
- Activity) Windows Event Log Analysis
- Activity) End of Section Review

SI3) Aggregation

- Section Introduction, Aggregation
- Log Aggregation Explained
- Activity) End of Section Review

SI4) Correlation

- Section Introduction, Correlation
- Normalization and Processing
- SIEM Rules
- Sigma Rules
- Regex
- Activity) Writing Sigma Rules
- Activity) End of Section Review

SI5) Using Splunk

- Section Introduction, Splunk
- Activity) Installing Splunk
- Activity) Installing BOTSv1 DatasetActivity)
- Splunk Crash Course - Users and Roles
- Splunk Crash Course - Navigation
- Splunk Crash Course - Search Queries
- Splunk Crash Course - Creating Alerts
- Splunk Crash Course - Creating Dashboards
- Activity) Splunk Scenario One
- Activity) Splunk Scenario Two

ABAD آباد
معهد شبكة آباد للتدريب
ABAD NETWORK FOR TRAINING

Domain 6: Incident Response (1/2)

IR1) Introduction

- Section Introduction, Incident Response
- What is Incident Response?
- Why is incident Response Needed?
- Security Events vs Security Incidents
- Incident Response Lifecycle
- CSIRT and CERT Explained
- Further Reading
- Incident Response Glossary
- Activity) End of Section Review

IR3) Detection & Analysis

- Section Introduction, Detection and Analysis
- Common Events and Incidents
- Using Baselines and Behavioural Profiles
- Introduction to Wireshark (GUI)
- Introduction to Wireshark (Analysis)
- Activity) PCAP 1
- Activity) PCAP 2
- Activity) PCAP 3
- YARA Rules for Detection
- Activity) Hunting With YARA
- CMD and PowerShell For Incident Response
- Activity) End of Section Review

SI2) Preparation Phase

- Section Introduction, Preparation
- Preparation: Incident Response Plan
- Preparation: Incident Response Teams
- Preparation: Asset Inventory and Risk Assessments
- Prevention: DMZ
- Prevention: Host Defences
- Prevention: Network Defences
- Activity) Setting up a Firewall
- Prevention: Email Defences
- Prevention: Physical Defences
- Prevention: Human Defences
- Prevention: Snort
- Activity) Deploying Snort
- Activity) End of Section Review

IR4) Containment, Eradication, Recovery

- Section Introduction, C.E.R
- Incident Containment
- Taking Forensic Images
- Identifying and Removing Malicious Artifacts
- Identifying Root Cause and Recovery
- Activity) End of Section Review

Domain 6: Incident Response (2/2)

IR5) Lessons Learned & Reporting

- Section Introduction, Lessons Learned
- What Went Well?
- What can be Improved?
- Important of Documentation
- Incident Response Metrics
- Reporting Format
- Report Considerations

IR6) MITRE ATT&CK

- Section Introduction, ATT&CK
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Activity) ATT&CK Navigator
- Activity) End of Section Review

Thank You!

ABAD أباد
معهد شبكة أباد للتدريب
ABAD NETWORK FOR TRAINING