ABAD أباد
معهد شبكة أباد للتدريب
ABAD NETWORK FOR TRAINING

معسكر المسار التأسيسي للأمن السيبراني

CyberSecurity Bootcamp Level 1

1 دورة CompTIA Network+

2 دورة CompTIA Security+

3 دورة CompTIA Linux+

4 دورة eJPT - Junior Penetration Tester

5 دورة BLUE TEAM LEVEL 1

1.0 Networking Concepts

1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.

- Layer 1 - Physical
- Layer 2 - Data link
- Layer 3 - Network
- Layer 4 - Transport
- Layer 5 - Session
- Layer 6 - Presentation
- Layer 7 - Application

1.2 Compare and contrast networking appliances, applications, and functions.

- Physical and virtual appliances
  - **Router**
  - **Switch**
  - **Firewall**
  - **Intrusion detection system (IDS)/intrusion prevention system (IPS)**
  - **Load balancer**
  - **Proxy**
  - **Network-attached storage (NAS)**
  - **Storage area network (SAN)**
  - **Wireless**
    - ▫ **Access point (AP)**
    - ▫ **Controller**
- Applications
  - **Content delivery network (CDN)**
- Functions
  - **Virtual private network (VPN)**
  - **Quality of service (QoS)**
  - **Time to live (TTL)**

1.3 Summarize cloud concepts and connectivity options.

- Network functions virtualization (NFV)
- Virtual private cloud (VPC)
- Network security groups
- Network security lists
- Cloud gateways
  - **Internet gateway**
  - **Network address translation (NAT) gateway**
- Cloud connectivity options
  - **VPN**
  - **Direct Connect**
- Deployment models
  - **Public**
  - **Private**
  - **Hybrid**
- Service models
  - **Software as a service (SaaS)**
  - **Infrastructure as a service (IaaS)**
  - **Platform as a service (PaaS)**
- Scalability
- Elasticity
- Multitenancy

1.4 Explain common networking ports, protocols, services, and traffic types.

Protocols	Ports
File Transfer Protocol (FTP)	20/21
Secure File Transfer Protocol (SFTP)	22
Secure Shell (SSH)	22
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name System (DNS)	53
Dynamic Host Configuration Protocol (DHCP)	67/68
Trivial File Transfer Protocol (TFTP)	69
Hypertext Transfer Protocol (HTTP)	80
Network Time Protocol (NTP)	123
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS)	443
Server Message Block (SMB)	445
Syslog	514
Simple Mail Transfer Protocol Secure (SMTPS)	587
Lightweight Directory Access Protocol over SSL (LDAPS)	636
Structured Query Language (SQL) Server	1433
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	5060/5061

- Internet Protocol (IP) types
  - **Internet Control Message Protocol (ICMP)**
  - **Transmission Control Protocol (TCP)**
  - **User Datagram Protocol (UDP)**
  - **Generic Routing Encapsulation (GRE)**
  - **Internet Protocol Security (IPSec)**
    - **Authentication Header (AH)**
    - **Encapsulating Security**
    - **Payload (ESP)**
    - **Internet Key Exchange (IKE)**
- Traffic types
  - **Unicast**
  - **Multicast**
  - **Anycast**
  - **Broadcast**

1.5 Compare and contrast transmission media and transceivers.

- Wireless
  - **802.11 standards**
  - **Cellular**
  - **Satellite**
- Wired
  - **802.3 standards**
  - **Single-mode vs. multimode fiber**
  - **Direct attach copper (DAC) cable**
    - **Twinaxial cable**
  - **Coaxial cable**
  - **Cable speeds**
  - **Plenum vs. non-plenum cable**
- Transceivers
  - **Protocol**
    - **Ethernet**
    - **Fibre Channel (FC)**
  - **Form factors**
    - **Small form-factor pluggable (SFP)**
    - **Quad small form-factor pluggable (QSFP)**
- Connector types
  - **Subscriber connector (SC)**
  - **Local connector (LC)**
  - **Straight tip (ST)**
  - **Multi-fiber push on (MPO)**
  - **Registered jack (RJ)11**
  - **RJ45**
  - **F-type**
  - **Bayonet Neill–Concelman (BNC)**

1.6 Compare and contrast network topologies, architectures, and types.

- Mesh
- Hybrid
- Star/hub and spoke
- Spine and leaf
- Point to point
- Three-tier hierarchical model
  - **Core**
  - **Distribution**
  - **Access**
- Collapsed core
- Traffic flows
  - **North-south**
  - **East-west**

1.7 Given a scenario, use appropriate IPv4 network addressing.

- Public vs. private
  - **Automatic Private IP Addressing (APIPA)**
  - **RFC1918**
  - **Loopback/localhost**
- Subnetting
  - **Variable Length Subnet Mask (VLSM)**
  - **Classless Inter-domain Routing (CIDR)**
- IPv4 address classes
  - **Class A**
  - **Class B**
  - **Class C**
  - **Class D**
  - **Class E**

1.8 Summarize evolving use cases for modern network environments.

- Software-defined network (SDN) and software-defined wide area network (SD-WAN)
  - **Application aware**
  - **Zero-touch provisioning**
  - **Transport agnostic**
  - **Central policy management**
- Virtual Extensible Local Area Network (VXLAN)
  - **Data center interconnect (DCI)**
  - **Layer 2 encapsulation**
- Zero trust architecture (ZTA)
  - **Policy-based authentication**
  - **Authorization**
  - **Least privilege access**
- Secure Access Secure Edge (SASE)/Security Service Edge (SSE)
- Infrastructure as code (IaC)
  - **Automation**
    - **Playbooks/templates/reusable tasks**
    - **Configuration drift/compliance**
    - **Upgrades**
    - **Dynamic inventories**
  - **Source control**
    - **Version control**
    - **Central repository**
    - **Conflict identification**
    - **Branching**
- IPv6 addressing
  - **Mitigating address exhaustion**
  - **Compatibility requirements**
    - **Tunneling**
    - **Dual stack**
    - **NAT64**

2.0 Network Implementation

2.1 Explain characteristics of routing technologies.

- Static routing
- Dynamic routing
  - **Border Gateway Protocol (BGP)**
  - **Enhanced Interior Gateway Routing Protocol (EIGRP)**
  - **Open Shortest Path First (OSPF)**
- Route selection
  - **Administrative distance**
  - **Prefix length**
  - **Metric**
- Address translation
  - **NAT**
  - **Port address translation (PAT)**
- First Hop Redundancy Protocol (FHRP)
- Virtual IP (VIP)
- Subinterfaces

2.2 Given a scenario, configure switching technologies and features.

- Virtual Local Area Network (VLAN)
  - **VLAN database**
  - **Switch Virtual Interface (SVI)**
- Interface configuration
  - **Native VLAN**
  - **Voice VLAN**
  - **802.1Q tagging**
  - **Link aggregation**
  - **Speed**
  - **Duplex**
- Spanning tree
- Maximum transmission unit (MTU)
  - **Jumbo frames**

2.3 Given a scenario, select and configure wireless devices and technologies.

- Channels
  - **Channel width**
  - **Non-overlapping channels**
  - **Regulatory impacts**
    - **802.11h**
- Frequency options
  - **2.4GHz**
  - **5GHz**
  - **6GHz**
  - **Band steering**
- Service set identifier (SSID)
  - **Basic service set identifier (BSSID)**
  - **Extended service set identifier (ESSID)**
- Network types
  - **Mesh networks**
  - **Ad hoc**
  - **Point to point**
  - **Infrastructure**
- Encryption
  - **Wi-Fi Protected Access 2 (WPA2)**
  - **WPA3**
- Guest networks
  - **Captive portals**
- Authentication
  - **Pre-shared key (PSK) vs. Enterprise**
- Antennas
  - **Omnidirectional vs. directional**
- Autonomous vs. lightweight access point

2.4 Explain important factors of physical installations.

- Important installation implications
  - **Locations**
    - **Intermediate distribution frame (IDF)**
    - **Main distribution frame (MDF)**
  - **Rack size**
  - **Port-side exhaust/intake**
  - **Cabling**
    - **Patch panel**
    - **Fiber distribution panel**
  - **Lockable**
- Power
  - **Uninterruptible power supply (UPS)**
  - **Power distribution unit (PDU)**
  - **Power load**
  - **Voltage**
- Environmental factors
  - **Humidity**
  - **Fire suppression**
  - **Temperature**

3.0 Network Operations

3.1 Explain the purpose of organizational processes and procedures.

- Documentation
  - **Physical vs. logical diagrams**
  - **Rack diagrams**
  - **Cable maps and diagrams**
  - **Network diagrams**
    - **Layer 1**
    - **Layer 2**
    - **Layer 3**
  - **Asset inventory**
    - **Hardware**
    - **Software**
    - **Licensing**
    - **Warranty support**
  - **IP address management (IPAM)**
  - **Service-level agreement (SLA)**
  - **Wireless survey/heat map**
- Life-cycle management
  - **End-of-life (EOL)**
  - **End-of-support (EOS)**
  - **Software management**
    - **Patches and bug fixes**
    - **Operating system (OS)**
    - **Firmware**
  - **Decommissioning**
- Change management
  - **Request process tracking/ service request**
- Configuration management
  - **Production configuration**
  - **Backup configuration**
  - **Baseline/golden configuration**

3.2 Given a scenario, use network monitoring technologies.

- Methods
  - **SNMP**
    - **Traps**
    - **Management information base (MIB)**
    - **Versions**
      - **v2c**
      - **v3**
    - **Community strings**
    - **Authentication**
  - **Flow data**
  - **Packet capture**
  - **Baseline metrics**
    - **Anomaly alerting/notification**
  - **Log aggregation**
    - **Syslog collector**
    - **Security information and event management (SIEM)**
  - **Application programming interface (API) integration**
  - **Port mirroring**
- Solutions
  - **Network discovery**
    - **Ad hoc**
    - **Scheduled**
  - Traffic analysis
  - **Performance monitoring**
  - **Availability monitoring**
  - **Configuration monitoring**

3.3 Explain disaster recovery (DR) concepts.

- DR metrics
  - **Recovery point objective (RPO)**
  - **Recovery time objective (RTO)**
  - **Mean time to repair (MTTR)**
  - **Mean time between failures (MTBF)**
- DR sites
  - **Cold site**
  - **Warm site**
  - **Hot site**
- High-availability approaches
  - **Active-active**
  - **Active-passive**
- Testing
  - **Tabletop exercises**
  - **Validation tests**

3.4 Given a scenario, implement IPv4 and IPv6 network services.

- Dynamic addressing
  - **DHCP**
    - **Reservations**
    - **Scope**
    - **Lease time**
    - **Options**
    - **Relay/IP helper**
    - **Exclusions**
  - **Stateless address autoconfiguration (SLAAC)**
- Name resolution
  - **DNS**
    - **Domain Name Security Extensions (DNSSEC)**
    - **DNS over HTTPS (DoH) and DNS over TLS (DoT)**
    - **Record types**
      - **Address (A)**
      - **AAAA**
      - **Canonical name (CNAME)**
      - **Mail exchange (MX)**
      - **Text (TXT)**
      - **Nameserver (NS)**
      - **Pointer (PTR)**
    - **Zone types**
      - **Forward**
      - **Reverse**
    - **Authoritative vs. non-authoritative**
    - **Primary vs. secondary**
    - **Recursive**
  - **Hosts file**
- Time protocols
  - **NTP**
  - **Precision Time Protocol (PTP)**
  - **Network Time Security (NTS)**

3.5 Compare and contrast network access and management methods.

- Site-to-site VPN
- Client-to-site VPN
  - **Clientless**
  - **Split tunnel vs. full tunnel**
- Connection methods
  - **SSH**
  - **Graphical user interface (GUI)**
  - **API**
  - **Console**
- Jump box/host
- In-band vs. out-of-band management

4.0 Network Security

4.1 Explain the importance of basic network security concepts.

- Logical security
  - **Encryption**
    - **Data in transit**
    - **Data at rest**
  - **Certificates**
    - **Public key infrastructure (PKI)**
    - **Self-signed**
  - **Identity and access management (IAM)**
    - **Authentication**
      - **Multifactor authentication (MFA)**
      - **Single sign-on (SSO)**
      - **Remote Authentication Dial-in User Service (RADIUS)**
      - **LDAP**
      - **Security Assertion Markup Language (SAML)**
      - **Terminal Access Controller Access Control System Plus (TACACS+)**
      - **Time-based authentication**
    - **Authorization**
      - **Least privilege**
      - **Role-based access control**
  - **Geofencing**
- Physical security
  - **Camera**
  - **Locks**
- Deception technologies
  - **Honeypot**
  - **Honeynet**
- Common security terminology
  - **Risk**
  - **Vulnerability**
  - **Exploit**
  - **Threat**
  - **Confidentiality, Integrity, and Availability (CIA) triad**
- Audits and regulatory compliance
  - **Data locality**
  - **Payment Card Industry Data Security Standards (PCI DSS)**
  - **General Data Protection Regulation (GDPR)**
- Network segmentation enforcement
  - **Internet of Things (IoT) and Industrial Internet of Things (IIoT)**
  - **Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT)**
  - **Guest**
  - **Bring your own device (BYOD)**

4.2 Summarize various types of attacks and their impact to the network.

- Denial-of-service (DoS)/ distributed denial-of-service (DDoS)
- VLAN hopping
- Media Access Control (MAC) flooding
- Address Resolution Protocol (ARP) poisoning
- ARP spoofing
- DNS poisoning
- DNS spoofing
- Rogue devices and services
  - **DHCP**
  - **AP**
- Evil twin
- On-path attack
- Social engineering
  - **Phishing**
  - **Dumpster diving**
  - **Shoulder surfing**
  - **Tailgating**
- Malware

4.3 Given a scenario, apply network security features, defense techniques, and solutions.

- Device hardening
  - **Disable unused ports and services**
  - **Change default passwords**
- Network access control (NAC)
  - **Port security**
  - **802.1X**
  - **MAC filtering**
- Key management
- Security rules
  - **Access control list (ACL)**
  - **Uniform Resource Locator (URL) filtering**
  - **Content filtering**
- Zones
  - **Trusted vs. untrusted**
  - **Screened subnet**

5.0 Network Troubleshooting

5.1 Explain the troubleshooting methodology.

- Identify the problem
  - **Gather information**
  - **Question users**
  - **Identify symptoms**
  - **Determine if anything has changed**
  - **Duplicate the problem, if possible**
  - **Approach multiple problems individually**
- Establish a theory of probable cause
  - **Question the obvious**
  - **Consider multiple approaches**
    - **Top-to-bottom/bottom-to-top OSI model**
    - **Divide and conquer**
- Test the theory to determine the cause
  - **If theory is confirmed, determine next steps to resolve problem**
  - **If theory is not confirmed, establish a new theory or escalate**
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and implement preventive measures if applicable
- Document findings, actions, outcomes, and lessons learned throughout the process

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.

- Cable issues
  - **Incorrect cable**
    - **Single mode vs. multimode**
    - **Category 5/6/7/8**
    - **Shielded twisted pair (STP) vs. unshielded twisted pair (UTP)**
  - **Signal degradation**
    - **Crosstalk**
    - **Interference**
    - **Attenuation**
  - **Improper termination**
  - **Transmitter (TX)/Receiver (RX) transposed**
- Interface issues
  - **Increasing interface counters**
    - **Cyclic redundancy check (CRC)**
    - **Runts**
    - **Giants**
    - **Drops**
  - **Port status**
    - **Error disabled**
    - **Administratively down**
    - **Suspended**
- Hardware issues
  - **Power over Ethernet (PoE)**
    - **Power budget exceeded**
    - **Incorrect standard**
  - **Transceivers**
    - **Mismatch**
    - **Signal strength**

5.3 Given a scenario, troubleshoot common issues with network services.

- Switching issues
  - **STP**
    - **Network loops**
    - **Root bridge selection**
    - **Port roles**
    - **Port states**
  - **Incorrect VLAN assignment**
  - **ACLs**
- Route selection
  - **Routing table**
  - **Default routes**
- Address pool exhaustion
- Incorrect default gateway
- Incorrect IP address
  - **Duplicate IP address**
- Incorrect subnet mask

5.4 Given a scenario, troubleshoot common performance issues.

- Congestion/contention
- Bottlenecking
- Bandwidth
  - **Throughput capacity**
- Latency
- Packet loss
- Jitter
- Wireless
  - **Interference**
    - **Channel overlap**
  - **Signal degradation or loss**
  - Insufficient wireless coverage
  - **Client disassociation issues**
  - **Roaming misconfiguration**

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

- Software tools
  - **Protocol analyzer**
  - **Command line**
    - **ping**
    - **traceroute/tracert**
    - **nslookup**
    - **tcpdump**
    - **dig**
    - **netstat**
    - **ip/ifconfig/ipconfig**
    - **arp**
  - **Nmap**
  - **Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP)**
  - **Speed tester**
- Hardware tools
  - **Toner**
  - **Cable tester**
  - **Taps**
  - **Wi-Fi analyzer**
  - **Visual fault locator**
- Basic networking device commands
  - **show mac-address-table**
  - **show route**
  - **show interface**
  - **show config**
  - **show arp**
  - **show vlan**
  - **show power**

CompTIA Security+

1.0 General Security Concepts

1.1-Compare and contrast various types of security controls.

1.2-Summarize fundamental security concepts.

1.3-Explain the importance of change management processes and the impact to security.

1.4-Explain the importance of using appropriate cryptographic solutions.

2.0 Threats, Vulnerabilities, and Mitigations

2.1-Compare and contrast common threat actors and motivations.

2.2-Explain common threat vectors and attack surfaces.

2.3-Explain various types of vulnerabilities.

2.4-Given a scenario, analyze indicators of malicious activity.

2.5-Explain the purpose of mitigation techniques used to secure the enterprise.

3.0 Security Architecture

3.1-Compare and contrast security implications of different architecture models.

3.2-Given a scenario, apply security principles to secure enterprise infrastructure.

3.3-Compare and contrast concepts and strategies to protect data.

3.4-Explain the importance of resilience and recovery in security architecture.

4.0 Security Operations

4.1-Given a scenario, apply common security techniques to computing resources.

4.2-Explain the security implications of proper hardware, software, and data asset management.

4.3-Explain various activities associated with vulnerability management.

4.4-Explain security alerting and monitoring concepts and tools.

4.5-Given a scenario, modify enterprise capabilities to enhance security.

4.6-Given a scenario, implement and maintain identity and access management.

4.7-Explain the importance of automation and orchestration related to secure operations.

4.8-Explain appropriate incident response activities.

4.9-Given a scenario, use data sources to support an investigation.

5.0 Security Program Management and Oversight

5.1-Summarize elements of effective security governance.

5.2-Explain elements of the risk management process.

5.3-Explain the processes associated with third-party risk assessment and management.

5.4-Summarize elements of effective security compliance.

5.5-Explain types and purposes of audits and assessments.

5.6-Given a scenario, implement security awareness practices.

CompTIA Linux+

Given a scenario, conduct software installations, configurations, updates, and removals

1. Package types

- .rpm
- .deb
- .tar
- .tgz
- .gz

2. Installation tools

- RPM
- Dpkg
- APT

3. Acquisition commands

- wget
- curl

Given a scenario, manage users and groups

1. Creation

- useradd
- groupadd

2. Modification

- usermod
- groupmod
- passwd
- chage

3. Deletion

- userdel
- groupdel

4. Important files and file contents

1. /etc/passwd
2. /etc/group
3. /etc/shadow

Given a scenario, create, modify, and redirect files

1. Text editors

- nano
- vi

2. File readers

- grep
- cat
- tail
- head
- less
- more

3. Output redirection

- - <<
- - >>
- - 2>
- - &>
- - stderr
- - /dev/null
- - /dev/tty
- - xargs
- - tee
- - Here documents
- <
- - >
- - |

·Given a scenario, create, modify, and redirect files

1. Text processing

- rep
- - tr
- - echo
- - sort
- - awk
- - sed
- - cut
- - printf
- - egrep
- - wc
- - paste

2. File and directory operations

- touch
- mv
- cp
- rm
- scp
- ls
- rsync
- mkdir
- rmdir

3. Given a scenario, manage services. Systemd management

- Systemctl
- Enabled
- Disabled
- Start
- Stop
- Mask
- Restart
- Status
- Daemon-reload
- Systemd-analyze blame
- Unit files
- Directory locations
- Environment parameters
- Targets
- Hostnamectl
- Automount
- Service
- Restart
- Status
- Stop
- Start
- Reload

·Given a scenario, apply or acquire the appropriate

1. File and directory permissions

- Read, write, execute
- - User, group, other
- - SUID
- - Octal notation
- - umask
- - Sticky bit
- - SGID
- - Inheritance
- - Utilities
- - chmod
- - chown
- - chgrp

2. Privilege escalation

- su
- - sudo
- - wheel
- - visudo
- - sudoedit

·Given a scenario, implement and configure Linux firewalls

1. Access control lists

- Source
- - Destination
- - Ports
- - Protocol
- - Logging
- - Stateful vs. stateless
- - Accept
- - Reject
- - Drop
- - Log

·Given a scenario, backup, restore, and compress files

1. Archive and restore utilities

- tar
- cpio
- dd
- Compression
- gzip
- xz
- bzip2
- zip

eJPT - Junior Penetration Tester

Assessment Methodologies: Information Gathering (1 Lab)

-Introduction To Information Gathering
-Passive Information Gathering
-Active Information Gathering

Assessment Methodologies: Footprinting & Scanning (5 Labs)

-Introduction
-Mapping a Network , Port Scanning
-Exercises
-Challenges

Assessment Methodologies: Enumeration (18 Labs)

-Introduction
-Overview
-SMB (7 Labs)
-FTP (2 Labs)
-SSH (2 Labs)
-HTTP (3 Labs)
-SQL (4 Labs)

Assessment Methodologies: Vulnerability Assessment (2 Labs)

-Introduction
-Vulnerability Overview
-Vulnerability Case Studies
-Nessus (1 Lab)
-Vulnerability Research (1 Lab)

Assessment Methodologies: Auditing Fundamentals (No Lab)

-Introduction
-Auditing Fundamentals

Host & Network Penetration Testing: System/Host Based Attacks (16 Labs)

-Introduction
-Host Based Attacks
-Windows Vulnerabilities
-Exploiting Windows Vulnerabilities (5 Labs)
-Windows Privilege Escalation (2 Labs)

Host & Network Penetration Testing: System/Host Based Attacks (16 Labs)

-Windows File System Vulnerabilities
-Windows Credential Dumping (2 Labs)
-Linux Vulnerabilities
-Exploiting Linux Vulnerabilities (4 Labs)
-Linux Privilege Escalation (2 Labs)
-Linux Credential Dumping (1 Lab)

Host & Network Penetration Testing: Network-Based Attacks (5 Labs)

-Introduction
-Tshark
-Wifi-Security

Host & Network Penetration Testing: The Metasploit Framework (MSF) (36 Labs)

-Introduction
-Metasploit Framework Overview
-Metasploit Fundamentals
-Information Gathering & Enumeration (2 Labs)
-Enumeration (7 Labs)
-MSF Vulnerability Scanning (1 Lab)
-Nessus Vulnerability Scanning
-Web Apps (1 Lab)
-Client-Side Attacks
-Windows Exploitation (3 Labs)
-Linux Exploitation (4 Labs)
-Post Exploitation Fundamentals (2 Labs)
-Windows Post Exploitation (10 Labs)
-Linux Post Exploitation (4 Labs)
-Metasploit GUIs (2 Labs)

Host & Network Penetration Testing: Exploitation (16 Labs)

-Introduction
-Introduction To Exploitation
-Vulnerability Scanning (2 Labs)
-Searching For Exploits
-Fixing Exploits (1 Lab)
-Bind & Reverse Shells (3 Labs)
-Exploitation Frameworks (1 Lab)

Host & Network Penetration Testing: Exploitation (16 Labs)

-Windows Exploitation (5 Labs)
-Linux Exploitation (4 Labs)
-AV Evasion & Obfuscation

Host & Network Penetration Testing: Post-Exploitation (26 Labs)

-Introduction
-Post-Exploitation
-Windows Local Enumeration (5 Labs)
-Linux Local Enumeration (5 Labs)
-Transferring Files To Windows & Linux Targets (3 Labs)
-Upgrading Shells (1 Lab)
-Windows Privilege Escalation (1 Lab)
-Linux Privilege Escalation (2 Labs)
-Windows Persistence (2 Labs)
-Linux Persistence (2 Labs)
-Dumping & Cracking Windows Hashes (1 Lab)
-Dumping & Cracking Linux Hashes (1 Lab)
-Pivoting Overview (1 Lab)
-Clearing Your Tracks (2 Labs)

Host & Network Penetration Testing: Social Engineering (1 Lab)

-Introduction
-Social Engineering Overview
-Let's Go Phishing (1 Lab)

Web Application Penetration Testing: Introduction to the Web and HTTP Protocol (12 Labs)

-Introduction
-Intro to Web
-web and http protocols
-HTTP Methods
-Directory Enumeration
-Burp Suite
-Nikto , vulnerabiltiy scanning
-SQLi with SQLMap
-XSS Attack with XSSer
-Attacking HTTP Login Form

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

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

A3) 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

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

SBT BLUE TEAM LEVEL 1

ABAD أباد
معهد شبكة أباد للتدريب
ABAD NETWORK FOR TRAINING

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 Dashboads
- Activity) Splunk Scenario One
- Activity) Splunk Scenario Two

SBT BLUE TEAM LEVEL 1

ABAD أباد
معهد شبكة أباد 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 Assessmen
- 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

ABAD آباد

معهد شبكة آباد للتدريب

ABAD NETWORK FOR TRAINING

☎ 920009129

www.abadnet.com.sa

✉ info@abadnet.com.sa