INTERNSETU
Code. Secure. Succeed.

LEARN
PRACTICE
HACK SECURELY
BUILD YOUR FUTURE

# ETHICAL HACKING

"THINK LIKE A HACKER TODAY SECURE THE ENTERPRISE TOMORROW"

THINK | HACK | DEFEND | SECURE

- RECON
- SCAN
- EXPLOIT
- REPORT
- DEFEND



TURNING VULNERABLITIES INTO STRENGTHENED DEFENSES

SKILLS FOR A OFFENSIVE SECURITY WORLD

INTERNSETU
Code. Secure. Succeed.

# ETHICAL HACKING
# LEARNING PATH

YOUR JOURNEY TO BECOME A CERTIFIED ETHICAL HACKER



RECON

SCAN

EXPLOIT

REPORT

DEFEND

## 01 YOU START HERE

Build your foundational knowledge in networking, Linux systems, and basic scripting.

> "THINK LIKE A HACKER TODAY, SECURE THE ENTERPRISE TOMORROW"

## 02 RECON & FOOTPRINTING

Master OSINT techniques, passive/active reconnaissance, and network scanning with Nmap.

## 03 VULNERABILITY ANALYSIS

Identify security flaws, unpatched systems, misconfigurations, and web vulnerabilities (OWASP Top 10).

## 04 SYSTEM & WEB EXPLOITATION

Safely exploit vulnerabilities using tools like Burp Suite, Metasploit, and custom exploit code.

## 05 PRIVILEGE ESCALATION & POST-EXPLOITATION

Escalate privileges on Windows/Linux, perform lateral movement, and analyze impact.

## 06 PENETRATION TESTER / SOC ANALYST

Write professional remediation reports, prepare for OSCP/CEH, and become job-ready.

TURNING VULNERABILITIES INTO **STRENGTHENED DEFENSES**

SKILLS FOR A **OFFENSIVE SECURITY** WORLD

INTERNSETU
Code. Secure. Succeed.

# ETHICAL HACKING & OFFENSIVE SECURITY

THINK HACK SECURE

## MASTER ENTERPRISE PENETRATION TESTING

FIND VULNERABILITIES | EXPLOIT BEFORE ATTACKERS | REMEDIATE & STRENGTHEN | BUILD A SECURE TOMORROW

"THINK LIKE A HACKER TODAY, SECURE THE ENTERPRISE TOMORROW"

## COURSE DESCRIPTION

Equip yourself with the offensive security mindset and technical skills needed to discover, exploit, and remediate critical security vulnerabilities before malicious actors can target them. This practical, hands-on course takes you step-by-step through the real-world penetration testing lifecycle—from initial reconnaissance and web application exploitation to internal network pivoting, privilege escalation, and executive reporting.

**TURNING VULNERABILITIES INTO STRENGTHENED DEFENSES**

## CORE LEARNING HIGHLIGHTS

### RECONNAISSANCE & FOOTPRINTING



Master OSINT gathering, network mapping, active host discovery, and port scanning with Nmap.

### WEB APPLICATION HACKING



Test for critical web vulnerabilities using Burp Suite, targeting the OWASP Top 10 (SQLi, XSS, CSRF, IDOR).

### NETWORK & SYSTEM EXPLOITATION



Leverage Metasploit, exploit public CVEs, perform password attacks, and bypass security controls.

### PRIVILEGE ESCALATION & POST-EXPLOITATION



Elevate privileges on Windows/Linux environments, move laterally across domains, and document findings.

HANDS-ON LABS | REAL-WORLD TOOLS | PRACTICAL SKILLS | CERTIFICATION PREP | JOB-READY EXPERTISE

INTERNSETU
Code. Secure. Succeed.

# OUR OBJECTIVES

## BUILD ROBUST ENTERPRISE DEFENSES & VULNERABILITY MANAGEMENT CAPABILITIES




IDENTIFY RISKS | IMPLEMENT CONTROLS | DETECT THREATS | STRENGTHEN DEFENSES

## PRIMARY GOAL

To empower security professionals with the skills required to identify system weaknesses, enforce defensive controls, and secure web applications and network infrastructure against **modern cyber threats**.

"FROM VULNERABILITIES TO A MORE SECURE TOMORROW"

## CORE LEARNING OBJECTIVES

### 01 MASTER DEFENSIVE FUNDAMENTALS & ARCHITECTURE

Understand network protocols, secure system configurations, and defensive concepts across enterprise environments.

### 02 CONDUCT VULNERABILITY ASSESSMENTS

Learn how to systematicallty scan, identify, and categorize security misconfigurations and software vulnerabilities using industry-standard tools.

### 03 SECURE WEB APPLICATIONS & INFRASTRUCTURE

Understand common web risks (such as the OWASP Top 10) and implement mitigation strategies, input validation, and secure coding practices.

### 04 IMPLEMENT SECURITY CONTROLS & INCIDENT PREPAREDNESS

Configure firewalls, intrusion detection systems (IDS), and logging frameworks to detect suspicious activity and respond effectively to security events.

PRACTICAL HANDS-ON SKILLS | REAL-WORLD SCENARIOS | INDUSTRY-RELEVANT KNOWLEDGE | JOB-READY SECURITY PROFESSIONALS

INTERNSETU
Code. Secure. Succeed.

# YOUR PATH

## From Security Foundations to Certified Defensive Expert

CERTIFIED DEFENSIVE EXPERT

LEARN → PRACTICE → BUILD SKILLS → GET CERTIFIED

CERTIFICATION
PRACTICE
SKILLS
FOUNDATION
DEFENSE
DEFENSE

## JOURNEY MILESTONES

### 01 PHASE 1 BUILD THE FOUNDATION

Grasp core networking protocols, Linux/Windows administration, OSINT gathering techniques, and zero trust security architecture.

### 02 PHASE 2 MASTER VULNERABILITY ASSESSMENT

Conduct system audits, perform network scans using Nmap, and identify software misconfigurations and unpatched vulnerabilities.

### 03 PHASE 3 IMPLEMENT DEFENSIVE CONTROLS

Harden web applications against OWASP Top 10 risks, configure firewalls, implement endpoint security, and enforce identity controls.

### 04 PHASE 4 OPERATIONAL READINESS & CERTIFICATION

Integrate SIEM log analysis, practice real-world incident response workflows, and prepare for industry certifications like Security+, CySA+, or Blue Team Level 1 (BTL1).

KNOWLEDGE
SKILLS
EXPERIENCE
CERTIFICATION
A SAFER TOMORROW

"STRONGER DEFENSES TODAY, A SAFER TOMORROW."

REAL-WORLD LEARNING | PRACTICAL HANDS-ON LABS | INDUSTRY-RELEVANT SKILLS | CERTIFICATION PREPARATION

INTERNSETU
Code. Secure. Succeed.

# COURSE PREREQUISITES

WHAT YOU NEED BEFORE STARTING YOUR DEFENSIVE SECURITY JOURNEY




RIGHT FOUNDATION | PRACTICAL KNOWLEDGE | REAL-WORLD READINESS | CONFIDENCE TO LEARN

## KEY REQUIREMENTS

### 01 NETWORKING FUNDAMENTALS

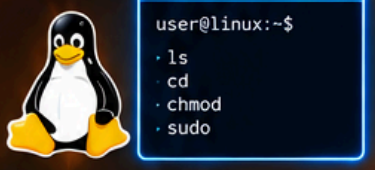
- Practical understanding of **TCP/IP**, **DNS**, **OSI model layers**, and common network protocols.
- Familiarity with basic **firewall rules**, **subnets**, and **routing concepts**.



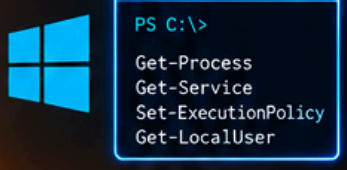
TCP/IP
DNS
OSI MODEL
FIREWALL
SUBNETS
ROUTING

### 02 OPERATING SYSTEM BASICS

- Foundational command-line navigation in both **Linux (Bash)** and **Windows (PowerShell/CMD)**.
- Basic knowledge of system administration, **file permissions**, and **user access management**.



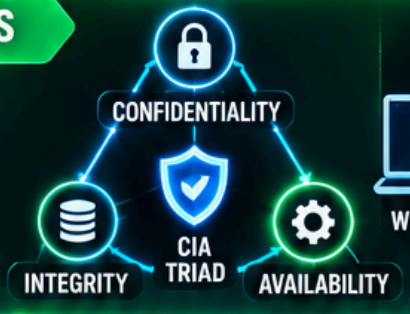

LINUX (BASH)

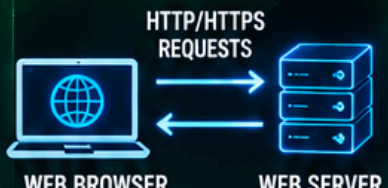



WINDOWS (POWERSHELL/CMD)

### 03 SECURITY & WEB AWARENESS

- Conceptual awareness of core security principles (**CIA Triad**: **Confidentiality**, **Integrity**, **Availability**).
- Understanding of how web browsers interact with web servers via **HTTP/HTTPS** requests.






INTERNSETU
Code. Secure. Succeed.

# KEY DEFENSIVE TOOLS & TECHNOLOGIES

Enterprise Blue Team Stack & Security Tooling




DETECT THREATS | ANALYZE RISKS | HARDEN SYSTEMS | RESPOND FASTER

## 1 RECONNAISSANCE, AUDITING & VULNERABILITY MANAGEMENT

Discover Assets. Identify Vulnerabilities. Reduce Attack Surface.

### Nmap & Masscan

NMAP | MASSCAN

- Industry-standard network mappers used for active host discovery, port scanning, and service version enumeration.

```
nmap -sV -sC 192.168.1.0/24
PORT     STATE   SERVICE
22/tcp   open    ssh
80/tcp   open    http
443/tcp  open    https
```

### Greenbone / OpenVAS & Nessus

Greenbone OpenVAS | nessus

- Enterprise vulnerability scanners used to automate system checks, detect unpatched software, and evaluate CVSS risk scores.




### OWASP ZAP & Burp Suite (Defensive Mode)

ZAP | Burp Suite

- Web application proxy tools used to identify web vulnerabilities (SQLi, XSS) and audit application security headers.

```
GET /api/user?id=1 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0
...
```

SQLi | XSS | Security Headers | IDOR

## 2 SIEM, MONITORING & SYSTEM HARDENING

Monitor Continuously. Detect Threats. Enforce Security Controls.

### Wazuh & Security Onion

Wazuh | Security Onion

- Open-source SIEM, host IDS (HIDS), and network security monitoring platforms used for centralized log aggregation and behavioral analysis.




### Splunk & Microsoft Sentinel

splunk> | Microsoft Sentinel

- Enterprise SIEM and SOAR platforms for threat detection, log correlation, and automated incident response workflows.




### CIS Benchmarks & Microsoft Intune / GPO

CIS Benchmarks | Microsoft Intune / GPO

- Hardening standards and enterprise configuration managers used to enforce OS baselines, firewall rules, and policy compliance.



INTERNSETU
Code. Secure. Succeed.

DETECT → ANALYZE → DEFEND

PEOPLE
PROCESS
TECHNOLOGY
VISIBILITY

DOMAIN 1

# SECURITY ARCHITECTURE & RECONNAISSANCE

Establishing Defensive Foundations and Threat Visibility




STRONG FOUNDATIONS | THREAT VISIBILITY | ATTACK SURFACE AWARENESS | PROACTIVE DEFENSES

"VISIBILITY TODAY, STRONGER DEFENSES TOMORROW"

## CORE LEARNING MODULES

### 1.1 ENTERPRISE SECURITY ARCHITECTURE

- The **CIA Triad**, Defense-in-Depth, and Zero Trust principles.
- Network segmentation, firewalls, and DMZ design fundamentals.
- Identity & Access Management (IAM) and Least Privilege enforcement.







### 1.2 PASSIVE RECONNAISSANCE & OSINT

- Gathering open-source intelligence on domain infrastructure safely.
- Analyzing publicly exposed assets, WHOIS records, and DNS records.
- Monitoring credential dumps and exposed cloud repositories.




- WHOIS RECORDS
- DNS RECORDS
- EXPOSED ASSETS
- CREDENTIAL DUMPS
- CLOUD REPOSITORIES

### 1.3 ACTIVE RECONNAISSANCE & ASSET DISCOVERY

- Mapping network perimeters and discovering live hosts using Nmap.
- Banner grabbing, service enumeration, and port scanning techniques.
- Documenting asset inventories to minimize unmanaged attack surfaces.

```
nmap -sS -sV 192.168.1.0/24

PORT      STATE   SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
3306/tcp  open    mysql
```

NMAP

HOST DISCOVERY | PORT SCANNING | SERVICE ENUMERATION | ASSET INVENTORY

PRACTICAL SKILLS | REAL-WORLD SCENARIOS | DEFENSIVE MINDSET | STRONGER SECURITY POSTURE

INTERNSETU
Code. Secure. Succeed.

DOMAIN 2

# VULNERABILITY ASSESSMENT & WEB DEFENSE

Identifying Flaws and Mitigating Web-Based Threats




DISCOVER VULNERABILITIES | ANALYZE RISKS | SECURE APPLICATIONS | BUILD STRONGER DEFENSES

"FIND THE FLAWS TODAY, BUILD STRONGER DEFENSES TOMORROW"

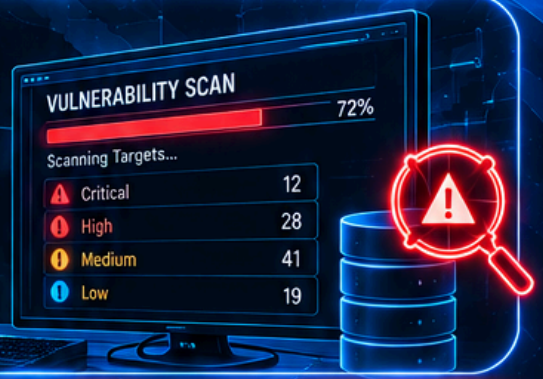
## CORE LEARNING MODULES

### 2.1 VULNERABILITY MANAGEMENT & SCANNING

- Automated vulnerability scanning using tools like OpenVAS and Nessus.
- Analyzing scan results, filtering false positives, and prioritizing CVEs.
- Common Configuration Enumeration (CCE) and Common Vulnerability Scoring System (CVSS).

OpenVAS

Nessus

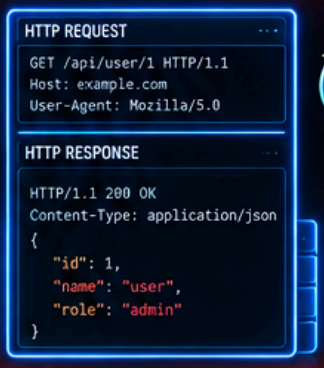



### 2.2 WEB APPLICATION SECURITY & OWASP TOP 10

- Understanding common web vulnerabilities: Injection (SQLi), Cross-Site Scripting (XSS), and Broken Access Control.
- Analyzing HTTP requests and responses using web proxies like OWASP ZAP.
- Reviewing API security risks and insecure direct object references (IDOR).

OWASP TOP 10

- SQL Injection
- Cross-Site Scripting (XSS)
- Broken Access Control
- Insecure Direct Object References
- API Security Risks




ZAP

### 2.3 WEB HARDENING & DEFENSE IMPLEMENTATION

- Input validation, output encoding, and parameterized queries.
- Configuring Web Application Firewalls (WAF) and security headers (CSP, HSTS).
- Implementing secure session management and multi-factor authentication (MFA).

WAF

- CSP
- HSTS
- X-Frame-Options
- Secure Cookies

MFA



PRACTICAL HANDS-ON LABS | REAL-WORLD TOOLS | DEFENSIVE KNOWLEDGE | JOB-READY SECURITY SKILLS

INTERNSETU
Code. Secure. Succeed.

DOMAIN 3

# SYSTEM HARDENING & DEFENSIVE CONTROLS

Securing Operating Systems, Endpoints, and Network Infrastructure




HARDEN SYSTEMS | CONTROL ACCESS | REDUCE ATTACK SURFACE | BUILD RESILIENT DEFENSES

## CORE LEARNING MODULES

### 3.1 OPERATING SYSTEM & ENDPOINT HARDENING

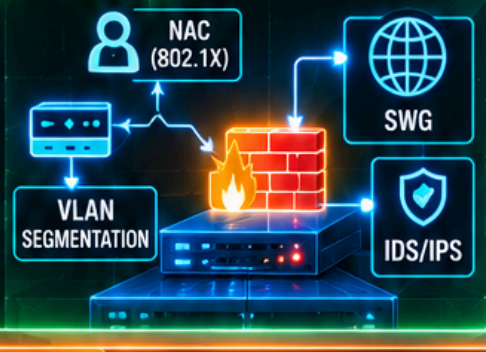
- Applying **CIS** (Center for Internet Security) **Benchmarks** and **DISA STIGs**.
- Disabling unnecessary services, ports, and legacy protocols (e.g., SMBv1, Telnet).
- Endpoint Detection and Response (**EDR**) deployment and host-based firewall policies.




- DISABLE UNNECESSARY SERVICES
- CLOSE UNUSED PORTS
- REMOVE LEGACY PROTOCOLS
- CONFIGURE HOST FIREWALL
- DEPLOY EDR

### 3.2 NETWORK DEFENSE & ACCESS CONTROL

- Configuring Network Access Control (NAC), VLAN segmentation, and 802.1X authentication.
- Implementing Secure Web Gateways (SWG) and Intrusion Detection/Prevention Systems (IDS/IPS).
- Securing administrative access via SSH keys, Jump Servers, and Privileged Access Management (PAM).




- NETWORK SEGMENTATION
- ACCESS CONTROL
- INTRUSION DETECTION / PREVENTION
- SECURE ADMIN ACCESS
- PRIVILEGED ACCESS MANAGEMENT (PAM)

### 3.3 PATCH & CONFIGURATION MANAGEMENT

- Establishing automated patch management workflows for OS and third-party software.
- Maintaining infrastructure configuration baselines using Infrastructure as Code (IaC) or Group Policy Objects (GPO).
- Mitigating supply chain risks through software bill of materials (SBOM) auditing.




- INFRASTRUCTURE AS CODE (IaC)
- GROUP POLICY OBJECTS (GPO)
- SBOM AUDITING

STRONGER INFRASTRUCTURE | PRACTICAL HANDS-ON LABS | INDUSTRY-STANDARD PRACTICES | JOB-READY SECURITY SKILLS

INTERNSETU
Code. Secure. Succeed.

DOMAIN 4

# INCIDENT RESPONSE & SIEM OPERATIONS

Continuous Monitoring, Threat Detection, and Remediation



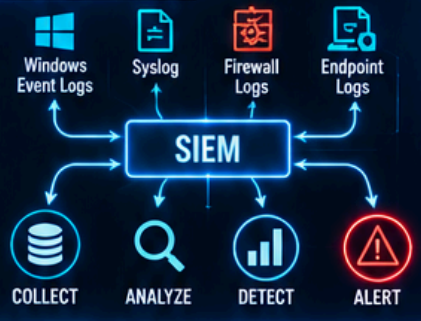

DETECT THREATS | RESPOND FASTER | MITIGATE IMPACT | BUILD A SAFER FUTURE

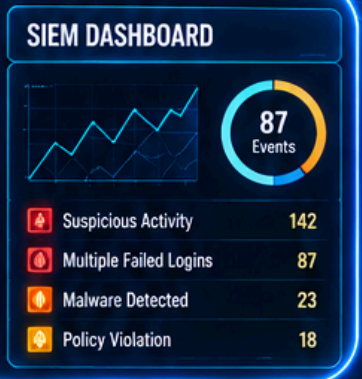
"FROM ALERTS TODAY TO A SAFER TOMORROW"

## CORE LEARNING MODULES

### 4.1 CENTRALIZED LOGGING & SIEM OPERATIONS

- Ingesting log sources (Windows Event Logs, Syslog, Firewall, Endpoint) into a centralized SIEM.
- Writing custom correlation rules and detection logic for suspicious activity.
- Monitoring dashboards for indicators of compromise (IoCs) and anomaly detection.

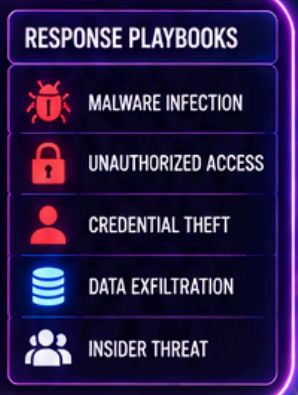



### 4.2 INCIDENT RESPONSE LIFECYCLE & PLAYBOOKS

- Following the NIST and SANS Incident Response frameworks (Preparation to Lessons Learned).
- Developing response playbooks for malware infections, unauthorized access, and credential theft.
- Performing containment, eradication, and system recovery procedures.




### 4.3 THREAT INTELLIGENCE & REMEDIATION REPORTING

- Leveraging open-source threat intelligence feeds (STIX/TAXII, MITRE ATT&CK Framework).
- Documenting incident timelines, root-cause analyses, and technical remediation steps.
- Communicating security findings and post-incident improvements to executive stakeholders.







"DETECT TODAY. RESPOND SMARTER. BUILD A SAFER TOMORROW"

REAL-WORLD | PRACTICAL | INDUSTRY FRAMEWORKS | DEFENSIVE | JOB-READY