Training Course on Web Shell Detection and Analysis

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's evolving threat landscape, web shells have emerged as one of the most insidious tools used by cybercriminals to exploit vulnerable web applications. These malicious scripts provide persistent backdoor access to compromised servers, enabling unauthorized remote control, data exfiltration, lateral movement, and stealthy attacks. As digital infrastructure expands, web shell detection and analysis have become a critical skillset for cybersecurity professionals, penetration testers, SOC analysts, and incident responders. Training Course on Web Shell Detection and Analysis provides comprehensive, hands-on knowledge required to identify, analyze, and mitigate these hidden threats using advanced tools and real-world techniques.

This instructor-led and lab-intensive course covers everything from code obfuscation patterns and command-and-control behavior to machine learning detection models and YARA-based threat hunting. Participants will develop an in-depth understanding of how attackers deploy web shells across various platforms such as PHP, ASP, JSP, and Python environments. By the end of the training, learners will be able to proactively hunt for and neutralize web shells, understand attacker TTPs (Tactics, Techniques, and Procedures), and integrate detection mechanisms into SIEMs, EDR, and cloud security solutions.

Programme Curriculum

Training Course on Web Shell Detection and Analysis

Introduction

In today's evolving threat landscape, web shells have emerged as one of the most insidious tools used by cybercriminals to exploit vulnerable web applications. These malicious scripts provide persistent backdoor access to compromised servers, enabling unauthorized remote control, data exfiltration, lateral movement, and stealthy attacks. As digital infrastructure expands, web shell detection and analysis have become a critical skillset for cybersecurity professionals, penetration testers, SOC analysts, and incident responders. Training Course on Web Shell Detection and Analysis provides

comprehensive, hands-on knowledge required to identify, analyze, and mitigate these hidden threats using advanced tools and real-world techniques.

This instructor-led and lab-intensive course covers everything from code obfuscation patterns and command-and-control behavior to machine learning detection models and YARA-based threat hunting. Participants will develop an in-depth understanding of how attackers deploy web shells across various platforms such as PHP, ASP, JSP, and Python environments. By the end of the training, learners will be able to proactively hunt for and neutralize web shells, understand attacker TTPs (Tactics, Techniques, and Procedures), and integrate detection mechanisms into SIEMs, EDR, and cloud security solutions.

Course Objectives

1. Understand web shell fundamentals and attack vectors
2. Identify commonly exploited web vulnerabilities leading to web shell deployment
3. Detect obfuscated malicious code in web environments
4. Analyze live and dormant web shell behavior using forensic techniques
5. Develop and deploy YARA rules for web shell detection
6. Use machine learning models for anomaly-based detection
7. Integrate web shell detection into SIEM and XDR systems
8. Perform memory and disk forensics to trace web shell activities
9. Conduct threat hunting using open-source intelligence (OSINT)
10. Automate web shell analysis using Python and custom scripts
11. Respond to web shell incidents using IR playbooks
12. Assess server hardening and mitigation best practices
13. Evaluate cloud-hosted application security against web shell threats

Target Audiences

1. Security Analysts
2. SOC (Security Operations Center) Teams
3. Incident Responders
4. Penetration Testers
5. Web Developers
6. IT Security Managers
7. Digital Forensics Experts
8. DevSecOps Professionals

Course Duration: 10 days

Course Modules

Module 1: Introduction to Web Shells

- Definition and history of web shells
- Common scripting languages used (PHP, ASP, JSP)
- MITRE ATT&CK framework techniques
- Web shell categories: single-function vs. full-featured
- Real-world impact on government and private networks
- **Case Study: China Chopper in a government agency compromise**

Module 2: Attack Vectors and Delivery Methods

- Exploited vulnerabilities: RCE, file upload flaws
- Web shell upload tactics
- Hidden extensions and filename spoofing

- Web application misconfigurations
- Lateral movement post-deployment
- **Case Study: Exploitation via CVE-2021-26855 (Exchange ProxyLogon)**

Module 3: Static Web Shell Detection

- Code pattern identification
- Obfuscation recognition
- Comparing hashes and known IOCs
- Regex and signature-based tools
- Static analysis automation tools
- **Case Study: Detecting obfuscated PHP shells on WordPress sites**

Module 4: Dynamic Behavior Analysis

- Sandbox execution and monitoring
- Behavioral profiling of web shells
- Logging suspicious HTTP requests
- API misuse detection
- Dynamic analysis frameworks
- **Case Study: Behavior monitoring on compromised IIS server**

Module 5: YARA Rules and Signature Creation

- Writing custom YARA rules
- Integrating YARA with file monitoring systems
- Rule tuning for false positive reduction
- Repositories of known web shell signatures
- Using VirusTotal with YARA
- **Case Study: Creating effective YARA rules for local web shell detection**

Module 6: SIEM and Log Correlation

- Integrating Apache/IIS logs into SIEM
- Log-based anomaly detection
- Triggering alerts for suspicious behaviors
- Threat intelligence enrichment
- Building correlation rules
- **Case Study: Correlating Splunk logs to identify persistent access**

Module 7: Memory Forensics

- Capturing volatile memory with tools like Volatility
- Extracting web shell indicators from RAM
- Analysis of injected code
- Malware persistence in memory
- Dealing with encrypted payloads
- **Case Study: Memory dump revealing encoded reverse shell**

Module 8: File System Forensics

- Timeline analysis of server files
- Metadata manipulation techniques
- Recovery of deleted web shells
- Directory traversal patterns
- File integrity monitoring

- **Case Study: Forensic analysis of .htaccess-controlled web shell**

Module 9: Cloud-Based Web Shells

- Exploitation in cloud apps (Azure, AWS)
- Containerized environments and risks
- Serverless function abuse
- Logging limitations in cloud
- Cloud-native security tools for detection
- **Case Study: Web shell in AWS Lambda due to S3 misconfig**

Module 10: Threat Hunting Techniques

- Developing web shell hunting hypotheses
- Leveraging OSINT for IOCs
- Using ElasticSearch and Kibana
- Filtering known-good traffic
- Prioritizing based on risk
- **Case Study: GitHub IOC leads to detection in live environment**

Module 11: Malware Analysis Automation

- Using Python for batch file analysis
- Integration with open-source tools (Cuckoo, ClamAV)
- Automated reporting dashboards
- Playbook scripting for detection
- Email and log-based triage automation
- **Case Study: Python script automating shell detection across 50 hosts**

Module 12: Incident Response for Web Shells

- Identification and containment steps
- Chain of custody for evidence
- IR team roles and escalation
- Mitigation of web shell persistence
- Legal and compliance considerations
- **Case Study: Multi-phase IR in retail breach with embedded web shell**

Module 13: Secure Development and Prevention

- Input validation and sanitization
- Secure coding standards (OWASP)
- Upload restriction techniques
- Web application firewalls (WAF)
- DevSecOps integration points
- **Case Study: Code audit reveals insecure file upload module**

Module 14: Advanced Machine Learning for Detection

- Supervised vs. unsupervised learning
- Feature extraction from web logs
- Model training with labeled datasets
- False positive management
- ML integration into SIEM
- **Case Study: ML model flags encoded ASPX web shell**

Module 15: Final Simulation and Capstone Project

- Full attack simulation with detection
- Forensics reporting and remediation planning
- Presenting findings to stakeholders
- Peer review of analysis
- Post-mortem and continuous monitoring
- **Case Study: Simulated cross-platform web shell attack lifecycle**

Training Methodology

- Instructor-led expert sessions with live Q&A
- Hands-on labs and simulations using real-world attack data
- Group exercises and collaborative analysis
- Guided threat hunting assignments
- Capstone project with red-blue team scenario

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com