CAk Cyber Akademie

SECTower
Fight against cyber attacks

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

CYBER DEFENCE SIMULATION TRAINING

Typische Angriffe auf Unternehmensnetze ganzheitlich verstehen

Im CYBER DEFENCE SIMULATION TRAINING werden IT-Angriffsmuster in realistischen IT-Umgebungen demonstriert.

Die Grundidee

In dem einmaligen Schulungskonzept werden typische IT-Angriffe im Kontext von „echten" Unternehmensnetzwerken simuliert.

Ziel ist, verschiedenste Angriffe auf Unternehmensnetzwerke unter Anleitung zu verstehen, zu erkennen und abzuwehren.

- Angreifer-Logik im Unternehmensnetzwerk verstehen.
- Grenzen von Sicherheitsprodukten richtig einschätzen.
- Härtungsmaßnahmen korrekt priorisieren.

Zielgruppen

Für wen ist das CYBER DEFENCE SIMULATION TRAINING geeignet?

- System- und Netzwerk-Administratoren
- IT-Security-Manager und -Entscheider
- Angehende Operations Engineers

Voraussetzungen

Es wird keine Hacking-Erfahrungen vorausgesetzt. Eine Affinität zum Thema IT-Security sollte allerdings vorliegen. Die nötigen Grundlagen werden zu Beginn des jeweiligen Kapitels ausführlich vermittelt.

Inhalt im Detail

Angriffe gegen IT-Unternehmensinfrastrukturen werden durch eine klassische „Red Team vs. Blue Team"-Demonstration simuliert:

- **Red Team – *Die Angreiferseite***
  Sie wird durch erfahrene SEC Consult Trainer simuliert.
- **Blue Team – *Die Verteidigerseite***
  Die Teilnehmer befinden sich hauptsächlich auf der Verteidigerseite. In verschiedensten Trainingsszenarien erlernen die Teilnehmer, Angriffe zu erkennen, zu stoppen und zu mitigieren.

Das Trainingssetup

Jeder Teilnehmer erhält Zugriff auf eigene IT-Infrastrukturen unter Nutzung von gängigen Standardprodukten, wie sie auch tagtäglich in Unternehmen zum Einsatz kommen:

- Windows-Domain-Struktur mit diversen Clients
- Windows- und Linux-Serversysteme
- Antiviren-Lösungen
- Web Application Firewalls (WAF)
- Sonstige IT-Monitoring- und SIEM-Lösungen

Die Agenda

Das Training behandelt die komplette **Attacker Kill Chain** von Anfang bis zum Ende. Dies beinhaltet folgende Schritte:

1. Reconnaissance
2. Initial Compromise
3. Establish Foothold
4. Escalate Privileges
5. Move Laterally
6. Complete Mission

Im Rahmen des Trainings werden folgende Themen im Detail auf technischer Ebene diskutiert und durch Do-It-Yourself Beispiele eigenständig durch die Teilnehmer vertieft:

- Windows-Domain-spezifische Sicherheit (Pass-The-Hash, etc.)
- Web-basierte Angriffe inklusive SQL Injektion, XSS und Weitere
- Privilege Escalation „zu Root" auf Windows- and Linux-Umgebungen
- Social Engineering mit bösartigen Anhängen
- Anti-Virus (AV) Bypasses
- Netzwerk-basierte Angriffe

„Nur wer moderne Angriffstechniken auf technischer Ebene versteht, kann erfolgreich Angriffe erkennen, abwehren, analysieren und langfristig verhindern."

Andreas Falkenberg

CAk Cyber Akademie

SECTower
Fight against cyber attacks

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Inhalt und Ablauf der Trainings – Red vs. Blue

Zeit	Tag 1 – Red vs. Blue	Tag 2 – Red vs. Blue	Tag 3 – Red vs. Blue
09.00–12.00 Uhr	1. **Awareness**	5. **Attacker Kill Chain: Initial Compromise Through Web Based Attacks** – XSS Schwachstellen – SQLi Schwachstellen – Datei-Uploads	8. **Attacker Kill Chain: Establish Foothold & Escalate Privileges on Windows Domain based Systems** – Windows-basierte Hash-Angriffe – Lokale „Privilege Escalations" – Windows-Netzwerk Pivoting-Angriffs
12.00–13.00 Uhr	Lunch	Lunch	Lunch
13.00–15.00 Uhr	2. **Einführung** – Einführung Training-Infrastruktur 3. **Hack-Like-A-Script-Kiddy** – Metasploit Tool Einführung	6. **Attacker Kill Chain: Establish Foothold & Escalate Privileges on Web Based Systems** – Verschiedene Root-Exploits auf Linux-Maschienen	8. **Attacker Kill Chain: Establish Foothold & Escalate Privileges on Windows Domain based Systems** – Anti-Virus (AV) Bypasses – Die Limitationen von Security-Produkten – Andere Netzwerk-basierte Angriffe 9. **Attacker Kill Chain: Complete Mission** – Diebstahl der „Kronjuwelen"
15.00–17.00 Uhr	4. **Attacker Kill Chain: Reconnaissance and the Limitations of Security Tools** – High Noise Scans – Low Noise Scans	7. **Attacker Kill Chain: Initial Compromise by (Spear)-Phishing Attacks** – Bösartige E-Mails – Social Engineering	10. **Crypto-Trojaner in Enterprise-Umgebungen** 11. **Outro**

Weitere Informationen erhalten Sie hier:

SEC Consult (Luxembourg) SARL
Frank Trenz
25, Avenue de la Gare
4131 Esch-sur-Alzette,
office-berlin@sec-consult.com
www.sectower.com

SEC Consult Deutschland Unternehmensberatung GmbH
Andreas Falkenberg
Ullsteinstr. 118, Turm B/8. Stock, 12109 Berlin
office-berlin@sec-consult.com
www.sec-consult.com

Cyber Akademie GmbH
Florian Lindemann
Kaskelstraße 41
10317 Berlin
info@cyber-akademie.de
www.cyber-akademie.de