

## Szkolenie

# Techniki hackingu i cyberprzestępczości - Poziom 4 Wyzwanie - zdobądź twierdzę

[Strona szkolenia](#) | [Terminy szkolenia](#) | [Rejestracja na szkolenie](#) | [Promocje](#)

## Opis szkolenia

Nadal pozostajemy w obszarze hackingu systemów i sieci, jednak zakres i możliwości są znacznie rozszerzone. Wychodzimy bowiem z założenia, że jeśli ktoś przeszedł już trzy edycje hackingu to posiada wystarczającą wiedzę, aby łączyć poznane techniki. Wraz z częścią czwartą szkolenia pojawią się komputery „twierdze”. Będą to specjalnie przygotowane systemy, które trzeba będzie „opanować”, zdobywając konto administratora wykorzystując wiedzę i techniki z poprzednich poziomów. Każdy dzień szkolenia będzie kończył się pełnym scenariuszem ataku, podczas którego uczestnicy będą łączyli poznane dotąd metody ataku na różne serwisy. Etap czwarty będzie posiadał również „wyzwanie” dla uczestników - od pierwszego dnia zostanie uruchomiony specjalny system, który będzie można atakować wszelkimi metodami. Celem będzie zdobycie konta głównego administratora.

## Wymagania

- Znajomość podstaw Linuxa, działania sieci, zasady działania systemów
- Wiedza ze szkolenia **Techniki hackingu i cyberprzestępczości - Poziom 1 Wprowadzenie do hackingu w praktyce**

## Program szkolenia

1. Nmap NSE Hardening
2. Systemy do analizy słabości serwisów sieciowych

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | [szkolenia@dagma.pl](mailto:szkolenia@dagma.pl)  
[szkolenia.dagma.eu](http://szkolenia.dagma.eu)

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15  
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy  
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł  
Numer NIP: 634-012-60-68, numer REGON: 008173852

3. Enumeracja i audytowanie ustawień systemu Linux
  4. Enumeracja i audytowanie ustawień systemu Windows
  5. Systemy automatyzujące testy bezpieczeństwa
  6. Haki na przeglądarkę użytkownika
  7. Hakowanie Wordpressa
  8. Hakowanie Joomla!
  9. Hakowanie baz danych MySQL
  10. Hakowanie serwera Tomcat
  11. Hacking Apache Struts - Remote Command Execution
  12. Hacking Apache Axis2
  13. Hacking Remote Services - SSH, FTP, SNMP
  14. Metody „odgadywania” haseł zaszyfrowanych plików
  15. Hacking and Discover User Account
  16. Zaawansowany Port Knocking jako zabezpieczenie przed exploitami i 0day
  17. Scenariusz ataku na system informatyczny - 1
  18. Scenariusz ataku na system informatyczny - 2
- 

## Tagi:

---

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | szkolenia@dagma.pl  
[szkolenia.dagma.eu](http://szkolenia.dagma.eu)

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15  
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy  
Numer KRS: 0000130206, kapitał zakładowy: 75 000 zł  
Numer NIP: 634-012-60-68, numer REGON: 008173852