Szkolenie

Techniki hackingu i cyberprzestępczości - Strony WWW i aplikacje webowe - poziom 2

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Warunkiem do przystąpienia do szkolenia wymagana jest wiedza zdobyta podczas szkolenia Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1.

Potrafisz już zaatakować i wybronić przed atakiem każdy system i każdą sieć? Młody padawanie - czas na mistrzowski poziom jedi!

Szkolenie Poziomu 2 poświęcone jest atakom na aplikacje webowe i strony www. Poznajemy metody atakowania i włamywania się do systemów informatycznych przez luki w oprogramowaniu WWW. Szkolenie odbywa się w specjalnie przygotowanym środowisku z kilkunastoma systemami, podatnymi na setki ataków najczęściej wykorzystywanych przez cyberprzestępców. Kończąc szkolenie masz kompleksową wiedzę z bezpieczeństwa IT, potrafisz też omijać i łamać zabezpieczenia serwerów WWW.

Korzyści po szkoleniu:

- Masz praktyczną wiedzę z zakresu bezpieczeństwa systemów operacyjnych oraz sieci informatycznych
- Znasz nowoczesne techniki internetowych włamywaczy
- Umiesz dobrać właściwe metody ochrony przed konkretnymi cyberatakami

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
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

Wymagania

- Znajomośc podstaw Linuxa, działania sieci, zasady działania systemów
- Wiedza ze szkolenia **Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1**

Harmonogram szkolenia

1. Wprowadzenie do tematyki ataków na strony internetowe i aplikacje webowe
2. Głębokie ukrycie
3. Insecure Logins Forms
4. Logout Management
5. Password Attack
6. Account Lockout
7. Web Parameter Tampering
8. Path oraz Information Disclosure
9. Path Traversal
10. Local File Inclusion
11. Remote File Inclusion
12. Omijanie filtrowania danych
13. Command Injection (+ Blind)
14. Sessions Management
15. Upload File
16. CSRF - Cross Site Request Forgery
17. SQL Injection - GET, POST
18. XSS Attack - Reflected, Stored
19. Automatyzacja SQL Injection

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
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