Szkolenie

Techniki hackingu i cyberprzestępczości - Poziom 5 PTH, eskalacje i obejście zabezpieczeń

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Wychodząc naprzeciw najbardziej wymagającym klientom, którzy oczekują sporej dawki wiedzy, adrenaliny i możliwości przetestowania swoich umiejętności, prezentujemy piątą część cyklu szkoleń nt. hackingu. Skupimy się w niej na PTH, eskalacji uprawnień w systemach Linux i Windows oraz szeroko rozumianym obejściu zabezpieczeń. Tym razem zajmiemy się także pozyskiwaniem haseł i tokenów z pamięci RAM, obejściem ograniczeń powłoki w systemie Linux oraz poznamy sposoby na deszyfrację haseł w systemach Windows. System Android również nie zostanie przez nas pominięty. Na deser zajmiemy się hakowaniem wirtualnych maszyn z poziomu gospodarza. Czyli jak włamując się na komputer utrzymujący wirtualizację włamać się do zasobów wirtualnego systemu. Poziom 5 to wyzwanie dla najwytrwalszych, zatem jeśli jesteś głodny technologicznych nowinek ze świata cyberprzestępczości- zapisz się już dziś!

Wymagania

- Znajomość podstaw Linuxa, działania sieci, zasady działania systemów
- Wiedza ze szkoleń **Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1** oraz **Techniki hackingu i cyberprzestępczości - Ataki na systemy i sieci** - to absolutne minimum! Jeżeli brałeś udział w całym cyklu szkoleń, jesteś idealnie przygotowany do przygody z najnowszą porcją wiedzy.

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
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Program szkolenia

1. Fingerprinting Internetu
2. Analiza szczegółowych informacji na temat firmy, osoby itp.
3. Raportowanie w NMAP-ie
4. Automatyzacja - zmiany wersji pythona napotrzeby określonych ataków
5. Tajemnice Respondera
6. CME - „szwajcarski scyzoryk” w analizach poeksploatacyjnych
7. Pozyskiwanie tokenów i haseł z pamięci RAM
8. Remote Code Execution w systemachWindows
9. Sposoby na poznanie haseł w systemach
10. Windows - Password Dumping
11. Eskalacja uprawnień w systemie Linux
12. Eskalacja w systemie Windows - Bypass UAC
13. Eskalacja uprawnień z wykorzystaniem perl-a
14. Obejście ograniczeń powłoki w systemie Linux
15. Scenariusze uzyskania uprawnień root
16. Podstawy hakowania systemu Android
17. Hakowanie maszyn wirtualnych z poziomu gospodarza
18. Hakowanie serwera Jenkins
19. Hacking Oracle GlassFish - Code Execution
20. Hacking Elasticsearch
21. Ukrywanie payloadow (zdjęcia, wizytówki)
22. Audyty bezpieczeństwa systemów Windows
23. Scenariusz ataku na system informatyczny - 1
24. 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

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.