

Poznaj nowe zastosowania języka Python!

Python to zaawansowany język programowania z ponad 20-letnią historią, który dzięki przemyślanej architekturze, ciągłemu rozwojowi i dużym możliwościom zyskał sporą sympatię programistów. Przełożyła się ona na liczbę dostępnych bibliotek i narzędzi wspierających tworzenie zarówno prostych, jak i skomplikowanych skryptów. Potencjał Pythona docenili również **pentesterzy** oraz inne osoby, którym nieobce są zagadnienia związane z

Jeżeli bezpieczeństwo systemów to Twoja pasja, to trafiłeś na doskonałą książkę! Sięgnij po nią i przekonaj się, jak szybko stworzyć w języku Python skrypt tropiący pakiety w systemach Windows i Linux, przeprowadzający **atak ARP** cache poisoning lub korzystający z **biblioteki urllib2**. Sporo uwagi zostało tu poświęcone tworzeniu koni trojańskich oraz budowaniu rozszerzeń dla **narzędzia Burp**. Możesz też sprawdzić, jak zaatakować przeglądarkę Internet Explorer oraz zdobyć wyższe uprawnienia w systemie Windows. Książka ta jest doskonałą lekturą dla czytelników chcących zbudować ciekawe narzędzia hakerskie przy użyciu języka Python.

Z książki tej dowiesz się, jak:

- Stworzyć trojana i sterować nim za pomocą konta w portalu **GitHub**

- Wykrywać ograniczone środowisko wykonawcze i automatyzować często wykonywane czynności, takie jak rejestrowanie naciskanych klawiszy i robienie zrzutów ekranu

- Zwiększać poziom uprawnień w systemie Windows przez sprytne sterowanie procesami

- Stosować ofensywne techniki analizy pamięci w celu **zdobycia haseł** i wstrzyknięcia kodu powłoki do maszyny wirtualnej

- Rozszerzać możliwości popularnego pakietu sieciowych **narzędzi hakerskich Burp Suite**

- Wykorzystywać funkcje **automatyzacji COM** systemu Windows do wykonywania **ataków typu „człowiek w przeglądarce”**

- Wykradać dane z sieci, nie ujawniając swojej działalności

Zbuduj własny, niezastąpiony pakiet narzędzi w języku Python!

O autorze (9)

O korektorach merytorycznych (10)

Przedmowa (11)

Wstęp (13)

Podziękowania (15)

1. Przygotowanie środowiska Pythona (17)

- Instalowanie systemu Kali Linux (18)

- WingIDE (20)

2. Podstawowe wiadomości o sieci (27)

- Narzędzia sieciowe Pythona (28)

- Klient TCP (28)

- Klient UDP (29)

- Serwer TCP (30)

- Budowa netcata (31)

 - Czy to w ogóle działa (37)

- Tworzenie proxy TCP (38)

 - Czy to w ogóle działa (43)

- SSH przez Paramiko (44)

 - Czy to w ogóle działa (47)

- Tunelowanie SSH (48)

 - Czy to w ogóle działa (51)

3. Sieć - surowe gniazda i szperacze sieciowe (53)

- Budowa narzędzia UDP do wykrywania hostów (54)

Tropienie pakietów w Windowsie i Linuksie (55)

 Czy to w ogóle działa (56)

Dekodowanie warstwy IP (57)

 Czy to w ogóle działa (60)

Dekodowanie danych ICMP (61)

 Czy to w ogóle działa (64)

4. Posiadanie sieci ze Scapy (67)

 Wykradanie danych poświadczających użytkownika z wiadomości e-mail (68)

 Czy to w ogóle działa (70)

 Atak ARP cache poisoning przy użyciu biblioteki Scapy (71)

 Czy to w ogóle działa (75)

 Przetwarzanie pliku PCAP (76)

 Czy to w ogóle działa (79)

5. Hakowanie aplikacji sieciowych (81)

 Internetowa biblioteka gniazd urllib2 (82)

 Mapowanie aplikacji sieciowych typu open source (83)

 Czy to w ogóle działa (84)

 Analizowanie aplikacji metodą siłową (85)

 Czy to w ogóle działa (88)

 Ataki siłowe na formularze uwierzytelniania (89)

 Czy to w ogóle działa (94)

6. Rozszerzanie narzędzi Burp (95)

 Wstępna konfiguracja (96)

 Fuzzing przy użyciu Burpa (96)

 Czy to w ogóle działa (103)

 Bing w służbie Burpa (107)

 Czy to w ogóle działa (111)

 Treść strony internetowej jako kopalnia haseł (113)

 Czy to w ogóle działa (116)

7. Centrum dowodzenia GitHub (119)

 Tworzenie konta w portalu GitHub (120)

 Tworzenie modułów (121)

 Konfiguracja trojana (122)

 Budowa trojana komunikującego się z portalem GitHub (123)

 Hakowanie funkcji importu Pythona (125)

 Czy to w ogóle działa (127)

8. Popularne zadania trojanów w systemie Windows (129)

 Rejestrowanie naciskanych klawiszy (130)

 Czy to w ogóle działa (132)

 Robienie zrzutów ekranu (133)

 Wykonywanie kodu powłoki przy użyciu Pythona (134)

 Czy to w ogóle działa (135)

 Wykrywanie środowiska ograniczonego (136)

9. Zabawa z Internet Explorerem (141)

 Człowiek w przeglądarce (albo coś w tym rodzaju) (142)

- Tworzenie serwera (145)
- Czy to w ogóle działa (146)
- Wykradanie danych przy użyciu COM i IE (146)
- Czy to w ogóle działa (153)

10. Zwiększanie uprawnień w systemie Windows (155)

- Instalacja potrzebnych narzędzi (156)
- Tworzenie monitora procesów (157)
 - Monitorowanie procesów przy użyciu WMI (157)
 - Czy to w ogóle działa (159)
- Uprawnienia tokenów Windows (160)
- Pierwsi na mecie (162)
 - Czy to w ogóle działa (165)
- Wstrzykiwanie kodu (166)
 - Czy to w ogóle działa (167)

11. Automatyzacja wykrywania ataków (169)

- Instalacja (170)
- Profile (170)
- Wydobywanie skrótów haseł (171)
- Bezpośrednie wstrzykiwanie kodu (174)
 - Czy to w ogóle działa (179)

Skorowidz (181)