

Spis treści

O autorze

O korektorze merytorycznym

Zespół wydania oryginalnego

Przedmowa

Wprowadzenie

Jak zorganizowana jest ta książka?

Dla kogo przeznaczona jest ta książka?

Podsumowanie

1 Czapka niewidka

Wprowadzenie

Badanie otwartych portów

Wprowadzanie w błąd skanera portów

Instalowanie pakietu knockd

Pakiety

Zmiana ustawień domyślnych

Zmiana lokalizacji plików

Niektóre opcje konfiguracyjne

Uruchamianie usługi

Zmiana domyślnego interfejsu sieciowego

Rodzaje pakietów i limity czasu

Testowanie zainstalowanego pakietu

Klienty port knocking

Ukrywanie serwera w sieci

Testowanie reguł zapory iptables

Zapisywanie reguł zapory iptables

Inne zagadnienia

Klienty działające na smartfonach

Diagnozowanie i usuwanie problemów

Bezpieczeństwo

Sekwencje efemeryczne

Podsumowanie

2 Cyfrowe odciski palców plików

Integralność systemu plików

System plików

Rootkity

Konfiguracja

Fałszywe alarmy

Przemyślany projekt

Podsumowanie

3 Netcat XXI wieku

Historia

Pakiety instalacyjne

Rozpoczynamy

Przesyłanie plików

Czat z użyciem programu ncat

Łączenie poleceń

Bezpieczna komunikacja

Pliki wykonywalne

Listy kontroli dostępu

Inne opcje

Podsumowanie

4 Odmowa działania usługi

Infrastruktura NTP

Ataki lustrzane z wykorzystaniem serwerów NTP

Raportowanie ataków

Zapobieganie atakom wykorzystującym odbicie SNMP

Serwery DNS

Współpraca

Powalić naród na kolana

Mapowanie ataków

Podsumowanie

5 Nping

Funkcjonalność

TCP

Interpreter

UDP

ICMP

ARP

Opcje ładunku

Tryb Echo

Inne opcje programu Nping

Podsumowanie

6 Analiza logów

Nieporozumienia związane z protokołem ICMP

Polecenie tcpdump

Zapora sieciowa iptables

Złożone reguły wieloczęściowe

Logowanie wszystkich połączeń do celów analizy śledczej

Utwarczanie systemu

Podsumowanie

7 Skrypty NSE pakietu Nmap

Podstawowe możliwości skanowania portów

Silnik skryptów programu Nmap

Szablony zależności czasowych skanowania

Kategorie skryptów NSE

Kryteria wyboru domyślnego zestawu skryptów

Luki w zabezpieczeniach

Testowanie uwierzytelniania

Wykrywanie hostów i usług

Aktualizowanie skryptów

Typy skryptów

Wyrażenia regularne

Graficzne interfejsy użytkownika

Zenmap

Podsumowanie

8 Wykrywanie złośliwego oprogramowania

Zaczynamy

- Częstotliwość aktualizacji bazy sygnatur

- Baza skrótów złośliwego oprogramowania

- Najczęściej występujące zagrożenia

- Funkcje i mechanizmy pakietu LMD

- Monitorowanie systemu plików

- Instalowanie pakietu LMD

- Tryby monitorowania

Konfiguracja

- Wyjątki

- Uruchamianie z poziomu wiersza poleceń konsoli

- Raportowanie

- Kwarantanna i naprawianie zainfekowanych plików

- Aktualizacja LMD

- Uruchamianie i zatrzymywanie skanowania

- Zadania cron

- Raportowanie wykrycia złośliwego oprogramowania

- Integracja z serwerem Apache

Podsumowanie

9 Łamanie haseł przy użyciu programu Hashcat

Historia

Zrozumieć hasła

Przestrzeń kluczy

Skróty haseł

Praca z programem Hashcat

Możliwości programu Hashcat

Instalacja pakietu

Identyfikacja skrótów

Wybieranie trybu ataku

Pobieranie słowników haseł

Tęczowe tablice

Uruchamianie programu Hashcat

oclHashcat

Hashcat-utils

Podsumowanie

10 Ataki z wykorzystaniem wstrzykiwania kodu SQL

Historia

Podstawy ataków typu SQL Injection

Zapobieganie atakom typu SQL Injection w kodzie PHP

Wykorzystywanie luk w SQL

Uruchamianie ataku

Gdzie można legalnie przeprowadzać ataki typu SQL Injection?

Podsumowanie