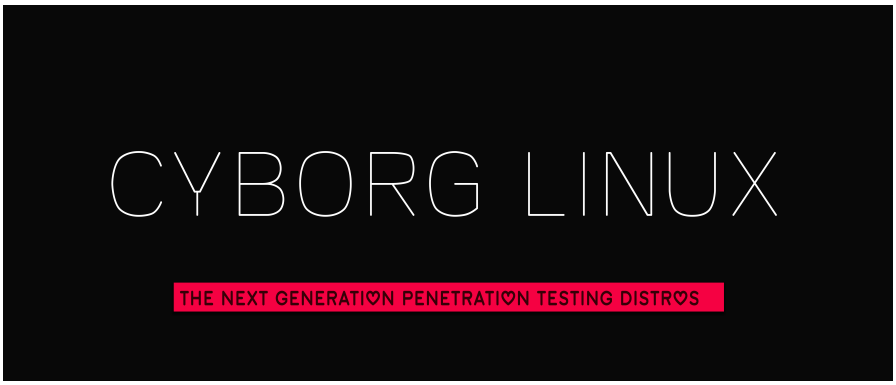
Cyborg Hawk Linux

Karolina Banasiewicz
Magdalena Oćwieja
Mahdi Maurycy El Khourani
Eryk Kozłecki

25 października 2016



Cyborg Hawk jest dystrybucją Linuxa, opartą na Ubuntu, stworzoną w celu przeprowadzania testów penetracyjnych. Zawiera wiele przydatnych narzędzi wykorzystywanych przez wielu specjalistów w celu testowania zabezpieczeń sieci, czy też w dziedzinach kryminalistyki cyfrowej i bezpieczeństwa urządzeń mobilnych. Jest to jedna z największych i najpopularniejszych dystrybucji tego typu na świecie.

1 Pobieranie i instalacja systemu

Strona domowa projektu:
http://cyborg.ztrela.com/

Całkowita waga systemu wynosi nieco ponad 3.1GB i w chwili obecnej jest dostępny wyłącznie w wersji 64-bitowej.

Latest version :

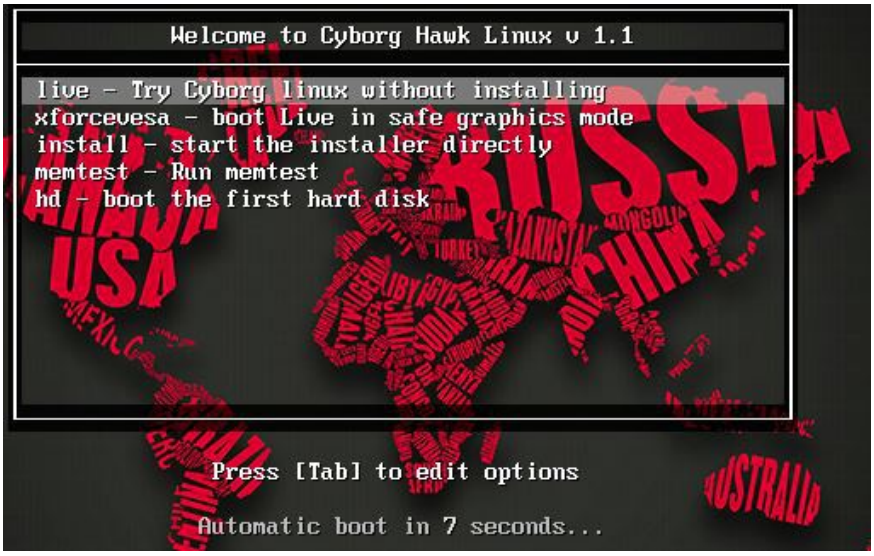
Download Cyborg Hawk v 1.1 :-

Currently there is 64 bit version of the distribution is available for download.

- To Download Click HERE

MD5 : fc87a403485b3b5ecbe63b0de9cb2327

System można bez problemu uruchomić z bootowalnego pendrive'a lub płyty LiveDVD.
Oczywiście możliwa jest bezpośrednia instalacja na dysku lub z wykorzystaniem maszyny wirtualnej - jest to dystrybucja Ubuntu, więc instalacja przebiega podobnie jak ma to miejsce w przypadku czystego systemu firmy Canonical.



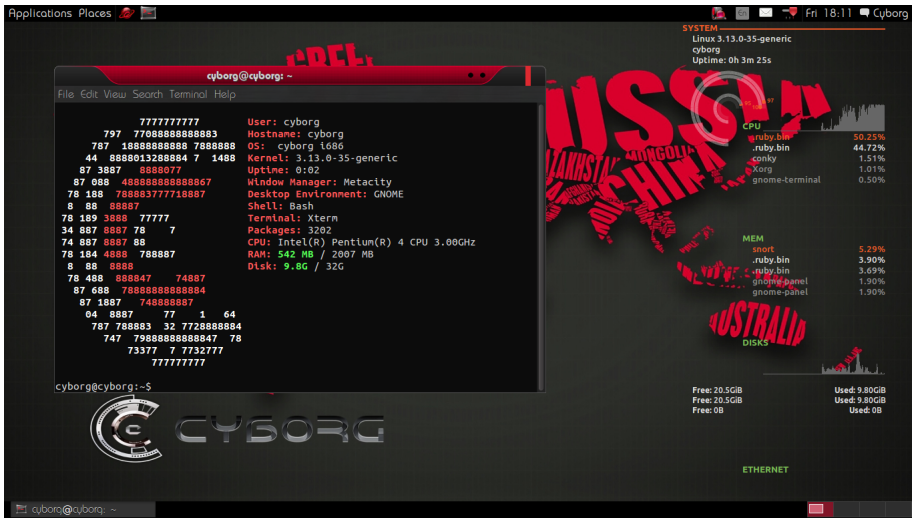
Obecna wersja systemu: Cyborg Hawk v 1.1

Domyślne dane logowanie dla systemu Cyborg Hawk:

- login: cyborg
- hasło: toor

2 Domyślny pulpit

Domyślny pulpit systemu został przedstawiony na poniższej grafice. W prawej części znajduje się widget prezentujący zużycie zasobów systemowych, co może okazać się niezwykle pomocne np. w trakcie skanowania dużej sieci.



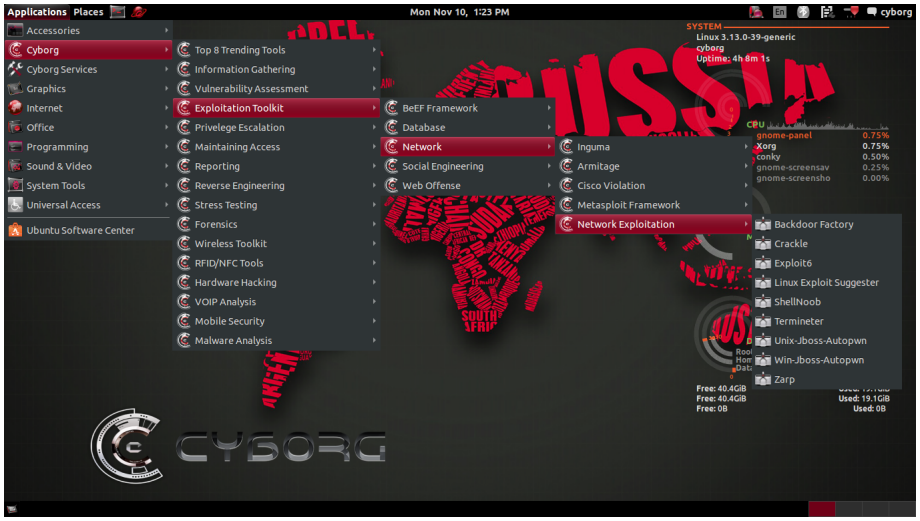
Sam interfejs jest bardzo prosty i przejrzysty - przypomina ten znany z wczesnych wersji Ubuntu bazujących na starszych wersjach środowiska graficznego Gnome.

3 Cyborg Hawk - dostępne narzędzia

Cyborg Hawk zawiera ponad 700 narzędzi wykorzystywanych przy szeroko rozumianych testach penetracyjnych podzielonych na następujące kategorie:

- Information Gathering - Gromadzenie danych
- Vulnerability Assessment - Ocena podatności
- Exploitation - Eksploatacja sieci
- Privilege Escalation - Eskalacja uprawnień
- Maintaining Access - Utrzymanie dostępu
- Documentation and Reporting - Raportowanie błędów i tworzenie dokumentacji
- Reverse Engineering - Inżynieria odwrotna
- Stress Testing

- Forensics - Informatyka śledcza
- Wireless Security - bezpieczeństwo sieci bezprzewodowych
- RFID/NFC - Analiza bezprzewodowych systemów komunikacji
- Hardware Hacking - M.in. analiza dysków twardych
- VoIP Analysis - analiza systemów VoIP
- Mobile Security - Bezpieczeństwo urządzeń przenośnych
- Malware Analysis - Analiza złośliwego oprogramowania



Cechy dystrybucji:

- Exploitation Toolkit- Tolkit służący do testowania spójności infrastruktury IT.
- Reverse Engineering- Zestaw narzędzi przeznaczonych do inżynierii odwrotnej.
- Forensics - Analiza cyfrowych dowodów popełnionych przestępstw.
- Stress Testing - Narzędzia służące do testowania urządzeń lub sieci będących pod dużym obciążeniem.
- Mobile Security:- Narzędzia penetracyjne testujące działanie zabezpieczeń w urządzeniach mobilnych
- Wireless Security:- Testowanie zabezpieczeń sieci bezprzewodowych.

Literatura

[1] http://www.darknet.org.uk/2016/03/cyborg-hawk-linux-penetration-testing-linux-distro/

[2] http://www.haxf4rall.com/2015/04/23/cyborg-hawk-linux-is-ready-to-take-on-kali/

[3] https://www.linux.com/blog/cyborg-hawk-linux