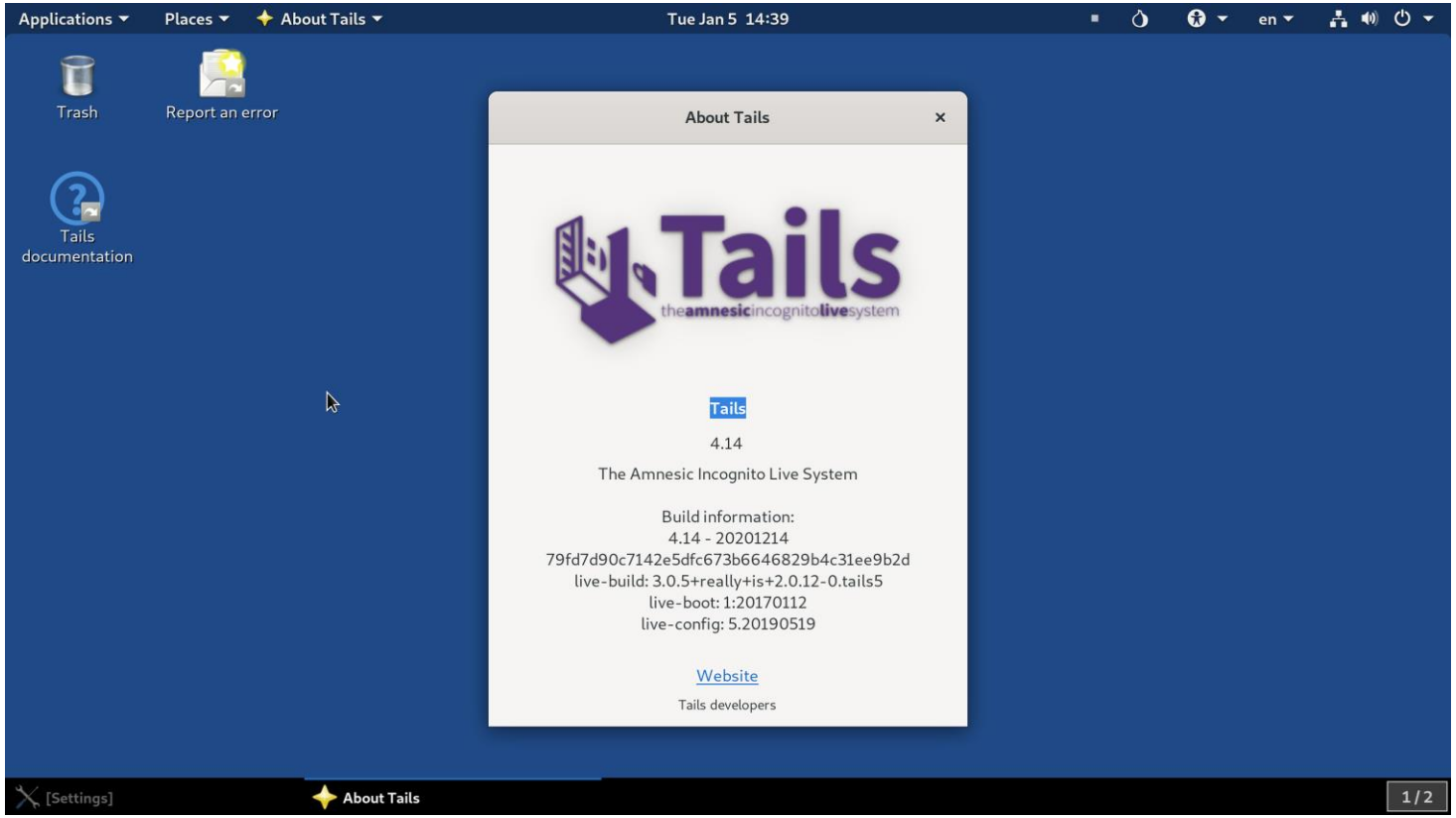
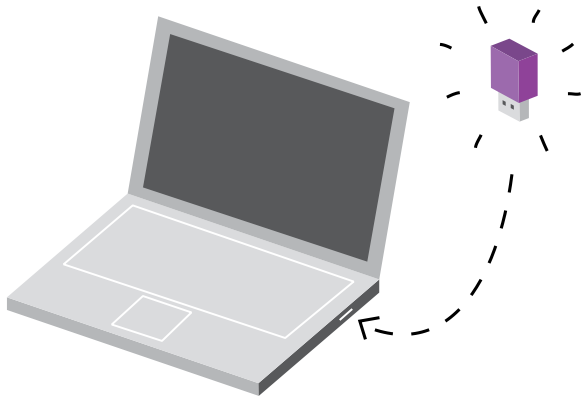
ARKADIUSZ ADAMCZYK
UTH RADOM

TAILS OS



OTWARTOŹRÓDŁOWA DYSTRYBUCJA LINUXA OPARTA NA DEBIANIE, SKUPIAJĄCA SIĘ NA ZACHOWANIU PRYWATNOŚCI I ANONIMOWOŚCI W SIECI

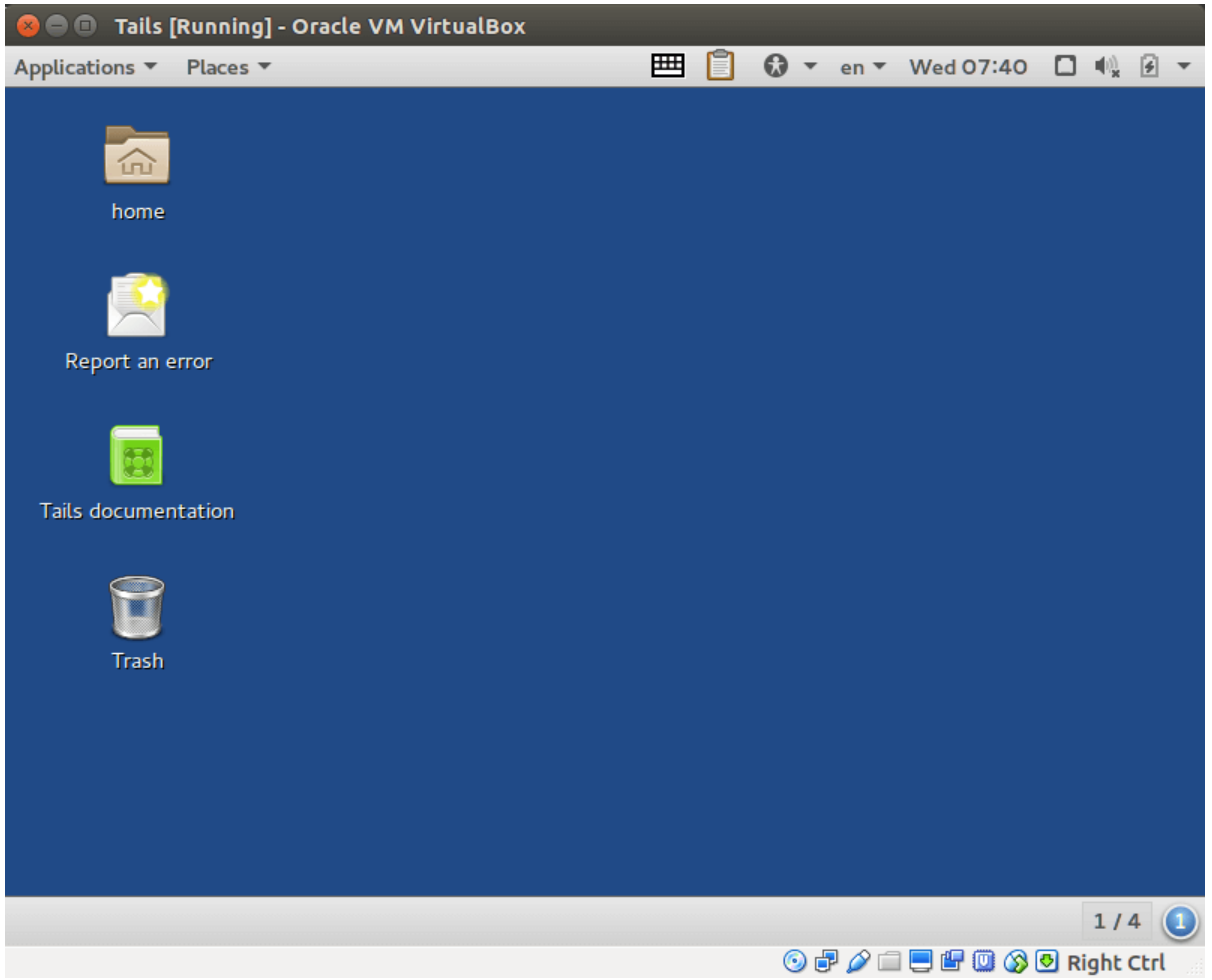
TAILS OS



CECHY

- PRZENOŚNOŚĆ (DZIAŁA W PAMIĘCI RAM I NIE ZAPISUJE NIC NA DYSKU)
- SZYFROWANIE POŁĄCZEŃ, BĄDŹ BLOKADA POŁĄCZEŃ Z ZEWNĄTRZ (FORSOWANYCH PRZEZ TOR'A)
- SZYFROWANIE ZAPISYWANYCH PLIKÓW
- WBUDOWANY ZESTAW SKONFIGUROWANYCH APLIKACJI

TAILS OS



BEZ PROBLEMU MOŻE DZIAŁAĆ JAKO GOŚĆ NA MASZYNIE WIRTUALNEJ

UŻYCIE / WYMAGANIA

POTRZEBNE:

PENDRIVE Z POJEMNOŚCIĄ MIN. 8GB

MIN. 2GB RAMU NA DOCELOWYM SPRZĘCIE

INSTALACJA:

POBIERZ TAILS'A

ZWERYFIKUJ PLIKI

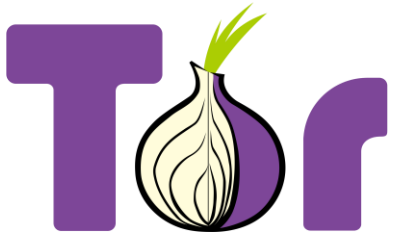
POBIERZ BALENAETCHER

ZAINSTALUJ TAILS'A UŻYWAJĄC BALENAETCHER

ZRESTARTUJ NA PENDRIVIE Z TAILSEM

VOILÀ!

APLIKACJE



COLD BOOT ATTACK

PODCZAS KORZYSTANIA Z KOMPUTERA, DANE ZAPISYWANE SĄ TYMCZASOWO W PAMIĘCI RAM (NP. HASŁA I KLUCZE SZYFRUJĄCE). IM BARDZIEJ NIEDAWNA AKTYWNOŚĆ, TYM WIĘKSZE PRAWDOPODOBIEŃSTWO, ŻE DANE NADAL SĄ W PAMIĘCI RAM

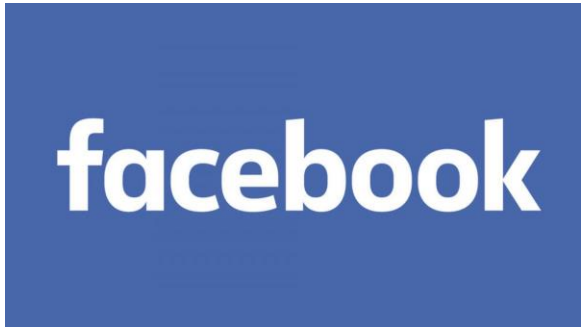
PO WYŁĄCZENIU KOMPUTERA DANE W PAMIĘCI SZYBKO ZNIKAJĄ, ALE MOGĄ POZOSTAĆ W NIEJ NAWET DO KILKU MINUT. OSOBA MAJĄCA DOSTĘP DO KOMPUTERA PRZED ICH CAŁKOWITYM ZNIKNIĘCIEM, MOGŁABY ODZYSKAĆ WAŻNE DANE Z SESJI. MOŻNA TO OSIĄGNĄĆ ZA POMOCĄ TECHNIKI ZWANEJ ***COLD BOOT ATTACK***

JEST TO PRZERYWANIE PRACY SYSTEMU NP. TWARDYM RESETEM, BY POTEM PRZY UŻYCIU PRZENOŚNEGO SYSTEMU ZROBIĆ ZRZUT ZACHOWANEJ PAMIĘCI RAM. ABY ZAPOBIEC TEMU ATAKOWI, DANE W PAMIĘCI RAM SĄ NADPISYWANE DANYMI LOSOWYMI PODCZAS ZAMYKANIA TAILS'A. WYMAZUJE TO ŚLADY Z SESJI UŻYTKOWNIKA NA TYM KOMPUTERZE

CIEKAWOSTKI

W ROKU 2014 WYSZŁO NA JAW, ŻE SYSTEM MASOWEJ INWIGILACJI XKEYSCORE OD NSA, OFLAGOWYWAŁ JAKO POTENCJALNE EKSTREMISTYCZNE ZAGROŻENIE KAŻDEGO, KTO POBIERAŁ, WYSZUKIWAŁ NAZWY LUB STRONY TAILSA. W ICH RAPORCIE RÓWNIEŻ TAILS ZOSTAŁ UZNANY ZA GŁÓWNE ZAGROŻENIE DLA ICH MISJI INWIGILACJI

CIEKAWOSTKI



W ROKU 2017 FBI WYKORZYSTAŁO ZŁOŚLIWY KOD OPRACOWANY PRZEZ FACEBOOKA, IDENTYFIKUJĄC SEKSUALNEGO SZANTAŻYSTE BUSTERA HERNANDEZA POPRZEZ LUKĘ ZERO-DAY W ODTWARZACZU WIDEO. EXPLOIT NIGDY NIE ZOSTAŁ ODKRYTY PRZEZ TWÓRCÓW TAILS'A, ALE UWAŻA SIĘ, ŻE LUKA ZOSTAŁA ZAŁATANA W PÓŹNIEJSZYM WYDANIU SYSTEMU.
BEZSKUTECZNE PRÓBY ZNALEZIENIA BUSTERA, ZMUSIŁY FBI DO STWORZENIA WŁASNEGO NARZĘDZIA HAKERSKIEGO TYLKO NA NIEGO, WYKORZYSTUJĄCEGO TĘ LUKĘ.

DZIĘKUJĘ ZA UWAGĘ

ARKADIUSZ ADAMCZYK
UTH RADOM

ŹRÓDŁA:

- https://tails.boum.org/
- https://en.wikipedia.org/wiki/Tails_(operating_system)
- GRAFIKI ODPOWIADAJĄCE LOGOM APLIKACJI