INFO DISTRO

BASATA SU
Debian Testing

PIATTAFORME SUPPORTATE
i386, amd64, ARM

RELEASING TYPE
Rolling Release

REQUISITI MINIMI
CPU: 1 GHz dual core
RAM: 384 MB
HDD: 16 GB

DISPLAY MANAGER
LIGHTDM

AMBIENTE DESKTOP
MATE

LICENZA
GNU/GPL v3

SITO WEB UFFICIALE
https:/www.parrotsec.org

Parrot security OS Linux all'italiana

Giunta alla sua **quarta versione**, è oggi una delle più popolari suite **GNU/Linux** del mondo pensate per l'**IT Security** e per l'**hacking**

Correva l'anno 2005 quando le prime distribuzioni per il Pentesting iniziarono a lasciare il segno nella vita di hacker intraprendenti. Gli anni d'oro per qualcuno, quando ancora i CD da 700MB erano l'unico limite all'immaginazione di una community sempre più in crescita: i tempi dei live CD da installare a fianco dei più blasonati Windows e OS X. Poi venne **Backtrack** che ancora oggi echeggia nella testa di chi è rimasto nel 2013. Cambiato nuovamente costume in **Kali**, la community hackerognola iniziò a guardare oltre la Offensive Security, a progetti alternativi e sicuramente affascinanti, tra cui le italianissime **Caine OS**, **Backbox OS** e **Parrot Security OS** di cui tratteremo in queste pagine. Diamo quindi un caloroso benvenuto alla distro del pennuto più acaro che c'è!

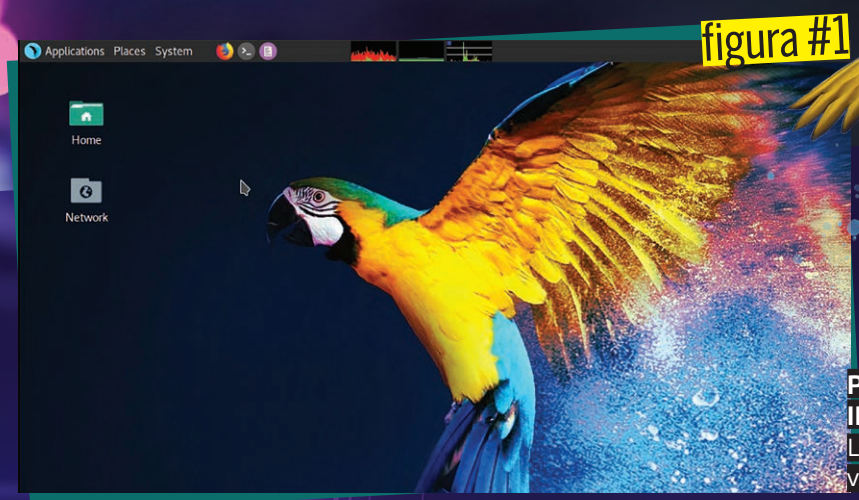


figura #1

PARROT SECURITY OS PENNUTO IN TUTTO IL SUO SPLENDORE!
Lo sfondo ufficiale delle ultime versioni è una esplosione di colori.

IL PENNUTO (MADE IN ITALY)

Parrot Security OS prende il nome da un iconico pappagallo che arieggia in ogni dove, dal sito web ufficiale (*https://www.parrotsec.org/*) al coloratissimo sfondo che da qualche versione a questa parte ci accompagna figura1.
L'intero progetto (da cui deriva non solo la distro ma anche altri servizi che a breve vi illustreremo) è coordinato da Lorenzo Faletra e dal suo team, i cui membri sono presenti in diverse realtà dell'ethical hacking italiano e non. Questa però è solo una piccola porzione che compone l'intero progetto Parrot: in ogni angolo del mondo troviamo volontari pronti a contribuire al progetto in maniera open source, sia come programmatori che come volontari per la scrittura di documentazione figura2.

CINQUE EDIZIONI PER PARROT OS

Parrot nasce prevalentemente come distribuzione GNU/Linux pensata per il pentesting, digital forensics, reverse engineering e lo sviluppo software. A queste si aggiungono ulteriori versioni che meritano certamente una considerazione a parte:

✓ **Home Edition:** la versione Parrot Home è destinata all'utente Parrot di tutti i giorni che è alla ricerca di una distribuzione leggera, sempre aggiornata (grazie al modello di aggiornamenti di tipo rolling release) e alla user-experience che contraddistingue questa distro. Sono inoltre inclusi tutti quei programmi pensati per la privacy e la sicurezza dell'utente, offrendo standard di crittografia elevati e strumenti di navigazione in incognito. È disponibile nelle versioni a 32bit e 64bit.
✓ **Studio Edition:** una versione "maggiorata" della Home, contenente una suite di programmi orientata alla produzione multimediale. Disponibile in versione 64bit.
✓ **Netinstall:** la versione ultra-leggera della ISO con cui è possibile crearsi la propria versione di Parrot scegliendo i packages che si preferiscono, mantenendo il core di Parrot e i vantaggi dello sterminato parco software a disposizione dell'utente. Disponibile per le architetture amd64, i386, arm64 e armhf.
✓ **Docker:** ecco una delle grandi novità di quest'anno. Sono distribuite ben tre tipologie di container hostabili (Core, Security e Metasploit) oltre ovviamente al codice sorgente con cui è possibile crearsi il proprio container su misura.
✓ **ARM:** tre versioni sperimentali dei principali "micro-computer" basati su architettura ARM (Raspberry, Orange Pi e Pine64), contenenti una versione ottimizzata di Parrot Security OS.

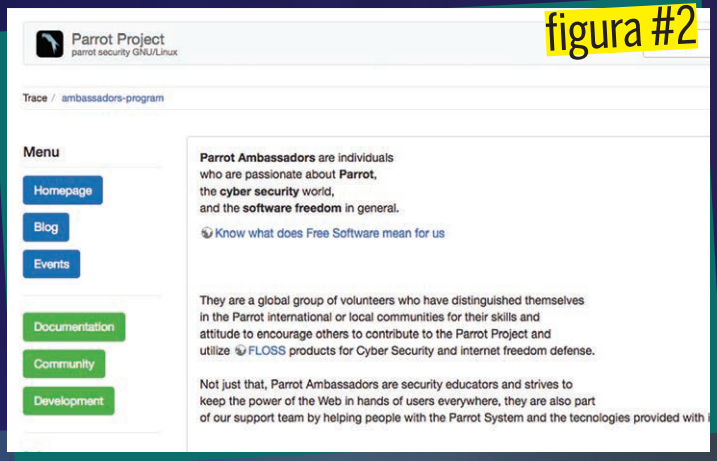


figura #2

figura #3

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] killing dangerous applications
[*] Dangerous applications killed
[*] cleaning some dangerous cache elements
[*] Cache cleaned

[ i ] Starting anonymous mode:


 * Stopping service nscd (already stopped)

 * Stopping service resolvconf
 * Stopping service dnsmasq (already stopped)
```

PAROLA D'ORDINE: SICUREZZA

Per quanto si possa considerare più o meno utile l'uso di tutti i giorni di una distribuzione pensata prevalentemente per l'IT Security, l'obiettivo principale del progetto Parrot rimane sempre lo stesso: offrire un ambiente pensato per la Sicurezza Informatica. E ci riesce alla grande, grazie alla decina di programmi preinstallati e configurati ad hoc, alla buona attività della community e degli sviluppatori che tengono in vita il progetto da ormai cinque anni.

UNA "MONTAGNA" DI TOOLS

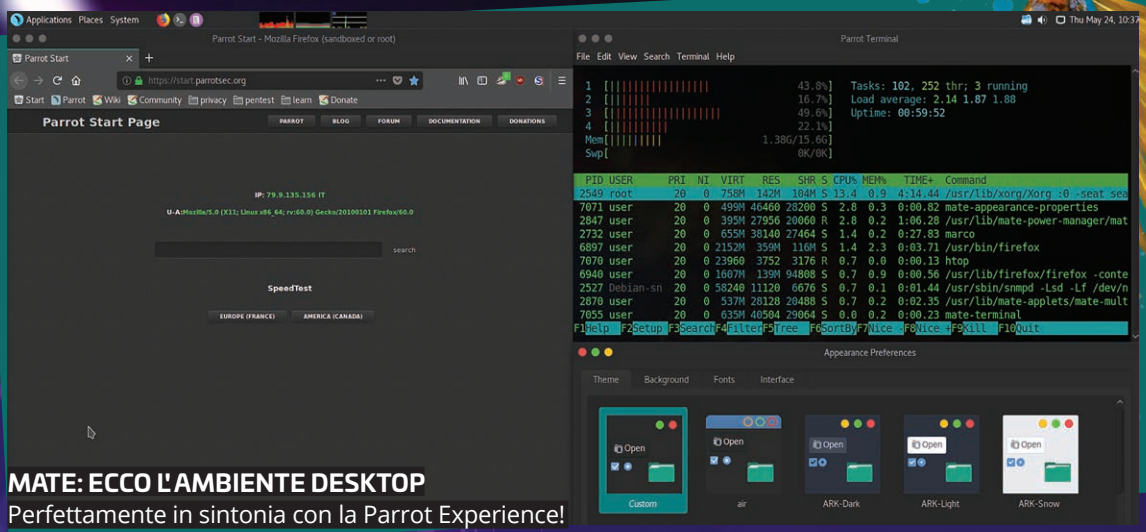
Se abbiamo già utilizzato una qualunque distro GNU/Linux di questo tipo probabilmente siamo già abituati a utilizzare un menu a navigazione diviso per categorie; di seguito elencheremo quelle presenti con una breve descrizione di ciò che contengono:

✓ **Information Gathering:** tool per effettuare raccolta di informazioni, OSINT, mappe concettuali, scanning di reti e sistemi e altro.
✓ **Vulnerability Analysis:** tool per effettuare il fingerprinting di un target specifico, identificare versioni e software in uso, generare report per la verifica manuale e molto altro
✓ **Web Application Analysis:** come prima ma pensato per il WWW e gli applicativi web
✓ **Database Assessment:** tools pensati per il management e il testing di (R)DBMS in generale
✓ **Exploitation Tools:** strumenti per effettuare intrusioni informatiche e ottenere l'accesso all'infrastruttura del target
✓ **Post Exploitation:** tool per aprirsi dei varchi nelle macchine vittima già compromesse per ottenere privilegi più elevati o creare sistemi di accesso persistente
✓ **Password Attacks:** tool per il cracking/bruteforcing di password cifrate
✓ **Wireless Testing:** tool per il pentesting verso reti Wi-Fi e verso altri protocolli wireless come Bluetooth e NFC/RFID o per dialogare con dispositivi SDR
✓ **Sniffing e Spoofing:** tool di intercettazione e manipolazione del traffico di rete
✓ **Digital Forensincs:** tool per la copia, l'estrazione e l'analisi forense di informazioni per investigazioni digitali o per uso giudiziario
✓ **Automotive:** tool dedicati all'hacking di automobili e dei network tipici del settore automotive

VUOI AGGIORNARE PARROT ALL'ULTIMA VERSIONE?

Se sei già il fiero possessore di un'installazione **Parrot Security OS** puoi aggiornarla facilmente lanciando i comandi:

```
$ sudo apt update
$ sudo apt purge tomoyo-tools
$ sudo apt full-upgrade
$ sudo apt autoremove
```



MATE: ECCO L'AMBIENTE DESKTOP
Perfettamente in sintonia con la Parrot Experience!

✓ **Reverse Engineering:** tool di debugging, reverse engineering, analisi e manipolazione di eseguibili
✓ **Reporting Tools:** tool per generare report sugli attacchi
✓ **System Services:** menu di accesso rapido per avviare e fermare servizi di sistema

ANON SURF, ANONIMATO FACILE FACILE

Da sempre uno dei punti di forza di questa distribuzione è stato Anon Surf, un servizio progettato specificatamente dal team di Parrot per garantire l'anonimato in rete figura3. Attraverso un semplice tool creato ad-hoc (attivabile sotto la voce Anon Surf dal menù in alto a sinistra) è possibile attivare questa modalità. La sua funzione sarà quindi quella di:

✓ Killare tutti i processi che potrebbero mettere a rischio la nostra identità
✓ Ripulire la cache in locale
✓ Stoppare eventuali servizi che potrebbero "ascoltare" le attività utente (nscd, resolvconf, dnsmasq etc...)
✓ Disabilitare i moduli IPv6
✓ Veicolare tutto il traffico sulla rete TOR

SANDBOX A GO-GO

Nell'universo dell'IT Security le sandbox consentono di chiudere ogni processo dentro un ambiente dedicato che risulta

Firejail consente di mettere in sandbox qualunque processo e anche la sessione utente

completamente isolato e dove vengono rese disponibili solo le risorse di cui quel programma ha bisogno. Immaginiamo che ogni volta che apriamo un programma una parte del nostro sistema venga clonata in un ambiente completamente isolato per far girare quel programma al suo interno, che tutti i potenziali danni causati da quel programma siano confinati dentro quella "scatola" e che questa venga distrutta alla fine dell'esecuzione di quel programma, salvando solo i dati persistenti.
Dalla versione 3.9, ma ufficializzato dalla 4.0, è Firejail, in combinazione con l'ormai celebre AppArmor a occuparsi di questo sporco lavoro: è un programma SUID in grado di "mettere in sandbox" qualunque tipo di processo: browser, tools CLI, editor di testo e anche la stessa sessione utente.
In questo modo, se qualcuno dovesse "bucare" un servizio in nostro possesso (come ad esempio succede con il web server in uso su Parrot), i danni al sistema verrebbero enormemente limitati.

COVER STORY: Gli italiani lo fanno meglio!

CERCHI UN'ALTERNATIVA?

Il mondo è bello perché è vario!
Se stiamo cercando una distribuzione GNU/Linux pensata per le nostre attività di IT Security consigliamo tre ottime distribuzioni completamente opensource:

- **Backbox:** *https://backbox.org/*
- **Caine OS:** *https://www.caine-live.net/*
- **Kali Linux:** *https://www.kali.org/*

AGGIORNAMENTI SOFTWARE

Tra le novità di minor rilievo, ma comunque degne di nota, troviamo **Nginx** come web server in sostituzione allo storico Apache; il pacchetto Apache2 sarà comunque presente nei repository o pre-installato per supportare alcuni tool. Aggiornato anche il **kernel** alla 4.16 con bugfix a Spectre e Meltdown e miglioramenti vari. L'ambiente Desktop **MATE** si aggiorna alla versione 1.20,viene introdotto **LibreOffice** 6 per il lavoro d'ufficio, mentre il browser **Firefox** avanza alla versione 60 beneficiando del salto prestazionale di cui tanto si è parlato. Concludiamo con il supporto all'**MD Raid**, che ora diventa di default ed è pronto per le nostre sessioni di Forensics!

TREND IN SALITA

Negli ultimi anni Parrot Security OS è diventata la seconda distribuzione GNU/Linux dedicata al Pentest più popolare su Distrowatch (*https://distrowatch.com*) figura4, ed è la 36esima distribuzione più scaricata di sempre. Con una media di 9.2 di score è tra le più adorate in assoluto!

figura #4

15	Kali	595 –
16	antiX	578 ▼
17	ReactOS	542 –
18	Lite	490 –
19	Endless	451 ▲
20	PCLinuxOS	442 –
21	Puppy	440 ▼
22	KDE neon	427 ▲
23	Lubuntu	426 –
24	deepin	378 ▼
25	Peppermint	374 –
26	Ubuntu MATE	365 –
27	SmartOS	353 –
28	Slackware	323 –
29	SparkyLinux	320 ▼
30	Xubuntu	312 –
31	Tails	307 ▼
32	Mageia	306 ▼
33	LXLE	295 –
34	ArchLabs	290 –
35	FreeBSD	276 –
36	Parrot	274 –

GLOSSARIO DI BASE

ROLLING RELEASE
Tipo di distribuzione GNU/Linux che segue uno schema di aggiornamenti a rilascio continuo senza "costringere" l'utente a effettuare un upgrade della distro in uso

ARCHITETTURE
Parrot Security OS è disponibile per diverse architetture: dalle classiche x86/x64 (per PC desktop e notebook) a quelle ARM (come i più recenti Raspberry Pi e micro-PC in generale)

CONTAINER
La nuova frontiera dell'isolamento informatico sostituisce le Virtual Machine. L'ecosistema viene fornito da Docker, una piattaforma opensource per Windows, Mac e GNU/Linux

"Ho iniziato per gioco, poi..."

IDENTIKIT

NOME: LORENZO FALETRA, IN ARTE "PALINURO"
PROFESSIONE: TEAM LEADER DI PARROT SECURITY
LUOGO DI NASCITA: PALERMO, ITALY

LINKEDIN:
https:/it.linkedin.com/in/lorenzofaletra

GITHUB:
https:/github.com/PalinuroSec

Quando (e come) ti sei avvicinato al mondo dell'IT Security?
Mi sono avvicinato relativamente tardi, verso i 14 anni, con un vecchio iMac g3 e con una Ubuntu 8.04 PPC senza interfaccia grafica. Data la scheda video leggermente fulminata, mi sono ritrovato costretto a usare il sistema interamente da shell e cominciare a giocare con vari linguaggi di programmazione.
La passione per l'IT security, nello specifico, è cominciata dalla lettura di un libro, "L'arte dell'hacking" di Jon Erickson, del quale, inizialmente, non ho capito assolutamente un accidente. Da lì è cominciato un percorso di studi ed esperimenti, parallelo alla lettura, col solo scopo di comprendere ogni parola criptica e nome di Pokemon che il testo mi proponeva. In questo modo è nata la mia passione per il mondo della sicurezza informatica.

Qual è stato il tuo percorso di studi per diventare un esperto nel settore?
La mia è la storia di un ragazzo completamente autodidatta che studiava networking e programmazione durante le lezioni di filosofia o latino, e coi compagni hackerini faceva le sfide di intrusione nei computer della scuola durante le ore di religione.
Acquisite le basi in modo del tutto sperimentale e casuale, mi sono reso conto di tanti errori di percorso e ho preso consapevolezza di molte mie lacune. Da lì è cominciato un percorso di studi, sempre privo di qualsiasi contributo da parte di enti scolastici o famiglia, organizzato in maniera piu strutturata che mi ha portato in pochi anni a cominciare a lavorare con gli standard di Debian e a sperimentare con dei primi esperimenti di distribuzione GNU/Linux customizzata.

Quando hai capito che era necessario creare Parrot?
In realtà il progetto è nato completamente per gioco come i 3 precedenti esperimenti di sviluppo di distribuzione.
Per me era fondamentale poter mettere una pendrive in qualsiasi computer e avere il mio ambiente coi miei programmi e le mie configurazioni già a bordo.
Il presupposto era che dover ricompilare una ISO ogni tot giorni per poter includere gli ultimi aggiornamenti, risolveva molti più problemi di quanti non ne causasse dover riconfigurare un intero sistema a ogni "formattone stagionale", e risolveva anche il problema di non avere il computer personale sempre a portata di mano.
Parrot OS, nello specifico, nasce come esperimento su Debian per avere un mio ambiente di pentest per sopperire a quelle che, dal basso della mia ignoranza da new entry dell'epoca, erano le lacune delle distro già esistenti, quali Backbox e Backtrack (che poco dopo venne soppiantata da Kali).
Da allora il progetto si è evoluto trasformandosi da un mero gioco a una distro usata da professionisti di vari settori, dall'IT security alla digital forensics.