

PREDATOR-OS ^{V 2.5}

SECURITY, PRIVACY, HARDENED, ANONYMIZED

Penetration Testing and Ethical Hacking

Polymorphic Security Platform



Developer: Hossein Seilani

1300 pre-installed tools which are split into 40 several categories

<https://predator-os.com/>

Linux Predator-OS

پلتفرم امنیتی چند وجهی

یک لینوکس منبع باز آزاد مبتنی بر امنیت

چکیده

توسعه آن در سال ۲۰۲۱ توسط [حسین سیلانی](https://emperor-os.com) که توسعه دهنده <https://emperor-os.com> نیز می باشد، آغاز شد. Predator-OS یک پروژه جامعه منبع باز آزاد، (مانند آزادی) است. این توزیع برای تست نفوذ و هک اخلاقی و همچنین حریم خصوصی، سخت شده، امن، لینوکس ناشناس است. Predator Linux مبتنی بر Ubuntu ۲۰،۰۴ LTS Mini هسته ۵،۱۸ LTS و با استفاده از یک دسکتاپ سبک وزن کاملاً سفارشی xfce۴ با منوی ویژه ابزارها است.

Predator Linux حدود ۱۰۰۰ ابزار از پیش نصب شده دارد که به ۴۰ دسته تقسیم می شوند. ابزارهای Predator از هر دو مخزن دبیان و اوبونتو و صفحه GitHub وارد می شوند. اکثر پیکربندی‌های هسته و کاربر به طور پیش فرض برای جلوگیری از هرگونه هک، دسترسی غیرمجاز و کاهش سطح حمله سفارشی سازی شده‌اند. بسیاری از فایروال‌های داخلی و ابزارهای دفاعی به کاربران نهایی اجازه می‌دهند تا Predator-OS را کنترل کنند. Predator همچنین از حریم خصوصی، ناشناس، ابزارهای امنیتی بسیار پشتیبانی می‌کند، و همچنین می‌تواند به صورت Live-CD یا از درایو USB و حالت نصب اجرا شود.

- نوع سیستم عامل: لینوکس
 - بر اساس: اوبونتو مینی ۲۰,۰۴ LTS
 - هسته: ۵,۱۸ LTS
 - اصل و نسب: تیم emperor-os
 - دسکتاپ: XFCE
 - دسکتاپ دیگر: به زودی: KDE plasma, mate, gnome
 - دسته بندی: تست نفوذ، امنیت، حریم خصوصی، پزشکی قانونی، رسانه زنده، سخت شده، ناشناس
- لینک دانلود:

<http://seilany.ir/predator-os/download/predator-os-v2.5-LTS.iso>

در ۹ حالت مختلف کار می کند:

Predator-OS دارای ۹ حالت مختلف است و در حالت های زیر برای دسترسی آسان و سریع تر به همه ابزارها کار می کند و همچنین می توان Linux Predator را در حالت های دفاعی، تهاجمی، حریم خصوصی، سخت شده، ایمن، تنظیمات و پیش آزمایش سریع تغییر داد.



Security
Mode



Offensive
Mode



Defensive
Mode



Anoninymied
Mode



Privacy
Mode



Tutorial
Mode



Emergency
Mode



Monitoring
Mode



Setting
Mode

ویژگی های جدید در Predator-OS

نسخه ۲,۵

ویژگی های جدید Predator-OS:

- (۱) دارای بیش از ۲ ترابایت لیست رمز عبور.
- (۲) دارای بیش از ۵۰۰ لیست از ابزارهای تیم قرمز و آبی است.
- (۳) دارای بیش از ۲۰۰ لیست از ابزارهای AWS-cloud.
- (۴) دارای بیش از ۱۰ مجموعه نقشه راه در امنیت سایبری
- (۵) دارای بیش از ۱۰۰ موتور جستجو در تست امنیت و نفوذ
- (۶) دارای بیش از ۳۰۰ اسکرپت آموزشی در تست امنیت و نفوذ
- (۷) دارای بیش از ۱۰۰ وب سایت آموزشی امنیتی و تست نفوذ برای کودکان.
- (۸) دارای بیش از ۱۰ ابزار برای اجرای آزمایشگاه امنیت سایبری و تست نفوذ
- (۹) دارای بیش از ۴۰ وب سایت برای اجرای آزمایشگاه در امنیت سایبری و تست نفوذ
- (۱۰) گنجانده شده به منبع ۸۰۰ فایل بدافزار در ۸۰ گروه مختلف (فایل ۴۰۰ مگابایت)
- (۱۱) دارای ۱۰۰۰ وب سایت برای OSINT.
- (۱۲) دارای بیش از ۷۰ وب سایت آنلاین و خودخوان در امنیت سایبری.
- (۱۳) دارای بیش از ۱۱ دسته آموزشی آفلاین و خودآموز در امنیت سایبری.
- (۱۴) دارای ۶۰۰ ابزار پزشکی قانونی و مهندسی معکوس.
- (۱۵) دارای بیش از ۶۰۰۰ dorks و اکسپلویت گوگل به صورت آفلاین

بهبود عملکرد و بهینه سازی سیستم در سطح هسته و سطوح کاربر:

- ۱) به منظور بهبود محدوده فرکانس CPU به طور پیش فرض intel_pstate به acpi-cpufreq تغییر یافته است.
- ۲) محدودیت فرکانس BIOS به طور پیش فرض غیرفعال شده است تا **performance** محدوده فرکانس CPU را بهبود بخشد.
- ۳) به منظور بهبود عملکرد هارد دیسک و زمان بوت شدن، Watchdog به طور پیش فرض غیرفعال شده است.
- ۴) بهبود عملکرد هارد دیسک با تغییر زمانبندی I/O برای دیسک های SATA، HDD و NVMe.
- ۵) بهبود عملکرد CPU با تغییر زمان بندی هسته پیش فرض به صورت هسته Linux-zen.
- ۶) بهبود عملکرد شبکه و اینترنت با تغییر پهنای باند تنگنا و زمان انتشار رفت و برگشت (BBR).
- ۷) بهبود عملکرد حافظه RAM با تغییر وضعیت randomize_va_space.
- ۸) بهبود عملکرد حافظه مجازی با جایگزینی zswap به جای swap به طور پیش فرض.
- ۹) رشته های سخت افزاری (CPU فیزیکی) برای هر هسته CPU فعال شده است.
- ۱۰) بهبود موازی وظایف با اجازه دادن به وظایف مستقل (رشته های در حال اجرا) با به اشتراک گذاری برخی منابع پردازنده.
- ۱۱) تغییر حالت صرفه جویی در مصرف انرژی به حالت **performance** به طور پیش فرض، به منظور بهبود عملکرد دیسک و IO شبکه.
- ۱۲) تمام فرکانس گاورنر CPU به **performance** سوئیچ شده است.
- ۱۳) کاهش گزارش های log-level هسته به سطح پایین به منظور بهبود عملکرد هسته و افزایش امنیت و ایجاد حالت بوت بی صدا.
- ۱۴) و همچنین، بهبود عملکرد TCP، افزایش حافظه کش اینود، کش دیسک، بهبود پارامترهای شبکه و پهنای باند و غیره.

ویژگی های برتر در Predator-OS

Predator-OS Linux دارای ویژگی های منحصر به فرد خود است که می توانید ۱۰۰ ویژگی را در سایت مشاهده کنید و همچنین دارای ویژگی هایی در مقایسه با توزیع های امنیتی است از جمله:

- ۱) نصب آسان و پشتیبانی سخت افزاری بهتر از توزیع کالی
- ۲) مناسب برای کاربران تازه کار و مفید برای کارهای عمومی در مقایسه با توزیع طوطی و کالی
- ۳) دارای تمام ابزارهای Parrot Linux
- ۴) با وجود ابزارهای بیشتر از توزیع Black Arch، حجم فایل دانلودی سبک تر و کمتر
- ۵) قابلیت بوت زنده و همچنین نصب در مقایسه با لینوکس ماهرانه با وجود داشتن تمامی ابزارهای این توزیع
- ۶) دارای ویژگی بوت شدن در حالت متن و داشتن ابزارهای CLI مانند توزیع dracOS است که فاقد ابزارهای گرافیکی است.
- ۷) تمام ابزارهای لینوکس Bugtraq را پوشش می دهد
- ۸) دارای ابزارهای تست نفوذ وب بیشتر از سامورایی لینوکس
- ۹) دارای ابزارهای بیشتری نسبت به BackBox Linux
- ۱۰) دارای تمام ابزارهای لینوکس Pentoo
- ۱۱) دارای ابزارهای تخصصی تشخیص جرم رایانه شخصی و همچنین امکان اجرای ابزارهای ویندوز در لینوکس مانند لینوکس ماهرانه و CAINE
- ۱۲) دارای ویژگی های لینوکس Kodachi در زمینه حفظ حریم خصوصی و ناشناس بودن است
- ۱۳) دارای ویژگی های امن و حریم خصوصی Linux Discreete
- ۱۴) دارای تمام ابزارهای لینوکس Santoku در زمینه Pentesting موبایل
- ۱۵) دارای ویژگی های توزیع Whonix برای امنیت بیشتر
- ۱۶) دارای تمام ابزارهای لینوکس Attifyos در زمینه تست نفوذ اینترنت اشیا و حتی بیشتر با رابط کاربر پسند
- ۱۷) دارای تمام ابزارهای stressLinux در زمینه تست استرس و موارد دیگر
- ۱۸) دارای ویژگی های ناشناس ماندن در وب مانند توزیع IprediaOS
- ۱۹) بسیاری از ابزارهای سایت زیر را پوشش دهید: insecure.org

شما می توانید تمام ۱۰۰ ویژگی لینوکس Predator-OS را در لینک زیر مشاهده کنید:

<https://predator-os.com/fich/index.html>

همه ۱۰۰ ویژگی Predator-OS

۱. توزیع لینوکس مبتنی بر امنیت

۲. Xfce به عنوان محیط دسکتاپ پیش فرض

۳. Operates در ۹ حالت های مختلف differnt

۴. به روز رسانی سیستم در قالب اسکریپت ساده و آماده

مدیر به روزرسانی هسته و ابزار، اعلان های به روزرسانی می توانند کاربر را در صورت قدیمی شدن سیستم خود مطلع کنند.

۵. مجموعه ابزارهای امنیتی

Predator Linux حدود ۱۳۰۰ ابزار از پیش نصب شده دارد که به ۴۰ دسته تقسیم می شوند

۶. سیستم بوت گرافیکی و لاگر

سیستم عامل دارای پلیموث است و می توانید برای مشاهده پیام کنسول، کلید پیکان را فشار دهید

۷. Live Mode به طور پیش فرض، Live DVD Live USB

همچنین، می توانید نصب کننده را اجرا کرده و آن را نصب کنید

XFce-Panel.۸

راه اندازهای برنامه، منوها، تعویض کننده فضای کاری و افزونه های بیشتر

Ulauncher.۹

یافتن و راه اندازی فایل های خود، باز کردن سریع وب سایت ها، یافتن برنامه ها و موارد دیگر بسیار آسان است.

۱۰. منوی سفارشی

Os اجازه دسترسی آسان و سریع به تمام برنامه های از پیش نصب شده را می دهد که به ۴۰ دسته تقسیم می شوند

ویژگی های ۱۱-۲۰

۱۱. ترمینال در پس زمینه دسکتاپ گرافیک بسیار قابل تنظیم، همیشه باز باشد و در پس زمینه دسکتاپ

۱۲. غیر فعال بودن **sleep**، **Hibernate**، **suspend**

به دلیل جلوگیری از دسترسی به کل حافظه و داده های خصوصی، رمزهای عبور، کلیدها

تهدید امنیتی

۱۳. ابزارهای حفظ حریم خصوصی

PrivacyTools، ابزار و دانشی را برای محافظت از حریم خصوصی شما در برابر نظارت گسترده جهانی ارائه می دهد.

۱۴. Fully OSINT Framword

تمرکز بر جمع آوری اطلاعات از ابزارها یا منابع رایگان

۱۵. ابزارهای باگ بانتهی

به کاربران این امکان را بدهید که از گروه بزرگی از هکرها استفاده کنند تا باگهای کدشان را پیدا کنند.

۱۶. دارای موتور جستجوی سایبری

موتورهای جستجوی خصوصی با ویژگی های محبوب و آخرین پیوندها

۱۷. ابزارهای CTF

اجرای یک ضبط، مسابقه پرچم (CTF)، ابزارهای مورد استفاده برای حل چالش های CTF

۱۸. آزمایشگاه تست نفوذ

ابزارهای زیادی برای یادگیری جنبه عملی ارزیابی آسیب پذیری و فضای مجازی برای آزمایش بدافزار وجود دارد

۱۹. اکثر درایورهای اسکندر

بیش از ۲۵۰۰ دستگاه اسکندر با بسته عاقل پشتیبانی می شود

۲۰. مرورگرهای با حفظ حریم خصوصی، مرورگر متمرکز بر حریم خصوصی، سپرهای برای

حفظ حریم خصوصی، مسدود کردن تبلیغات مضر

ویژگی های ۲۱-۳۰

۲۱. ابزار چت گروهی امن دارای برنامه پیام رسانی ایمن است. رمزگذاری انتها به انتها، پیام رسانی چند حالته، پشتیبانی از چند پلتفرم

۲۲. ابزار خود تخریبی

هر گزارش، آهنگ، حافظه، حافظه پنهان و خاموش کردن سریع کامپیوتر را پاک کنید

تهدید امنیتی ۲۳. ابزار VPN

همه ارتباطات داده را ایمن کنید و شبکه خصوصی را گسترش دهید. از طریق یک اتصال رمزگذاری شده به شبکه شرکتی ایمن دسترسی پیدا کنید

۲۴. SHELL هوشمند و کاربر پسند

دارای zsh و پوسته ماهی

۲۵. Included IDS/IPS Tools

آنتی ویروس، حذف تروجان، شناسایی بدافزار، AIDE، SELinux، apparmor و فایروال ها

۲۶. ابزارهای بررسی یکپارچگی

دارای ابزارهایی برای مقایسه وضعیت داده های ذخیره شده و نظارت بر یکپارچگی فایل

۲۷. Apparmor Profiles

تمام نمایه‌های apparmor موجود را نصب و فعال کرد

۲۸. دارای ابزار محافظ USB

جلوگیری از یواس بی، دسترسی فیزیکی و حملات الکتریکی

۲۹. Included Tune ابزار

ابزار خط فرمان تنظیم شده به کاربران اجازه می دهد بین پروفایل های تنظیم مختلف جابجا شوند.

۳۰. ابزار نظارت بر زمان واقعی

نظارت و عیب یابی همه چیز در زمان واقعی به صورت رایگان با Netdata

ویژگی های ۳۱-۴۰

۳۱. پایگاه داده هک گوگل

شما می توانید به بیش از ۶۰۰۰ دورک گوگل دسترسی داشته باشید

۳۲. controlling همه خدمات دارای ابزار Stacer برای کنترل همه سرویس ها

۳۳. حذف داده های غیر ضروری

حذف سرویس ها، بسته ها، فایل های راه اندازی و تنظیمات غیر ضروری

۳۴. [Ctrl]-[Alt]-[Delete] را غیرفعال است.

به هر کسی اجازه راه اندازی مجدد سیستم عامل با استفاده از کلیدهای Ctrl-Alt-Del داده نشده است.

۳۵. Included Database Tools دارای مفیدترین ابزارهای مدیریت پایگاه داده است

۳۶. دارای ابزار حسابرسی

دارای ممیزی امنیتی و ابزار تشخیص نفوذ: بپر، lynis و ابزارهای بیشتر

۳۷. دارای پروتکل های Mix Networks

ارتباطات سخت ردیابی، با رمزگذاری و ناشناس نگه داشتن شما در اینترنت. مانند OpenVPN، Tor، ایزپ، فانوس

۳۸. دارای osquery

به شما امکان می دهد پرس و جوهای سیستم خود را با استفاده از دستورات SQL برای عیب یابی عملکرد و مشکلات عملیاتی ایجاد کنید

۳۹. دارای ابزار مدیریت ورود به سیستم

مدیریت و تجزیه و تحلیل فایل های گزارش، ثبت فعالیت های سیستم، رویدادها و ابزارهای تولید گزارش

۴۰. لیست های رمز عبور

دسترسی به لیست گذرواژه ۳۰۰ گیگابایتی حاوی هر فهرست لغت، فرهنگ لغت و پایگاه داده رمز عبور است

ویژگی های ۴۱-۵۰

۴۱. دارای ابزار پاک کردن اطلاعات به طور کامل از هارد دیسک، حافظه، بازنویسی بخش و پاک کردن کش

۴۲. دارای صفحه کلید مجازی

فلورانس یک صفحه کلید مجازی مقیاس پذیر با منبع باز است

۴۳. جعبه ابزار تجزیه و تحلیل بدافزار دارای جعبه ابزار برای مهندسی معکوس و تجزیه و تحلیل ویندوز و لینوکس مخرب، محققان قانونی

۴۴. یادگیری ماشین برای امنیت سایبری دارای python ۲ و ۳ ماژول برای InfoSec، تجزیه و تحلیل بدافزار، امنیت سایبری و

یادگیری ماشین است.

۴۵. ابزارهای سند متنوع

۴۶. مدیریت بسته

دارای **apt**، **aptitude**، **alein**، **synaptic**، **snap**، **dpkg**

۴۷. تنظیم هسته دارای تنظیمات تنظیم هسته مانند حافظه پنهان، مشخصات عملکرد تنظیم شده است.

۴۸. دارای ابزارهای **cpupower**

دارای مجموعه ای از ابزارها برای بررسی و تنظیم ویژگی های مربوط به صرفه جویی در مصرف انرژی پردازنده شما.

۴۹. ابزارهای بازیابی اطلاعات

دارای ابزارهایی برای از دست دادن داده ها، اطلاعات حیاتی یا از طریق حذف تصادفی، حملات ویروسی، حذف دائمی داده های خراب فایل ها

۵۰. **Metapackage Forensic**

همه ابزارهای موجود در اینجا توسط تیم ابزار امنیتی دبیان بسته بندی شده اند

ویژگی های ۵۱-۶۰

۵۱. دارای مجموعه Sleuth Kit از ابزارهای خط فرمان برای تجزیه و تحلیل تصاویر دیسک و بازیابی فایل ها از آنها

۵۲. ExecShield سرریز بافر

محافظت در برابر سرریز بافر

۵۳. ایمن سازی دسترسی به شبکه

در برابر سیل بسته های syn و حملات ARP محافظت می شود

۵۴. غیرفعال کردن خودکار نصب

ویژگی نصب خودکار درایوهای متحرک را خاموش است.

۵۵. فولدرهای مشترک ماشین مجازی غیرفعال شده است

غیرفعال کردن نصب ماشین مجازی پوشه های مشترک بین میزبان و مهمان

۵۶. کاربر عادی به عنوان Default

از کاربر عادی به عنوان Default استفاده می کنید، اکانت روت را برای همیشه غیرفعال کنید و دستور را با sudo اجرا کنید

۵۷. رمزگذاری

دارای ابزارهای رمزگذاری متقارن و نامتقارن برای فایل ها و حجم ها

۵۸. دارای ASLR

Address Space Layout Randomization.all randomization از سوء استفاده از آسیب پذیری های تخریب حافظه جلوگیری می کند

۵۹. سازگار و ماشین های مجازی X۸۶

پشتیبانی از ماشین های مجازی و سازگار با X۸۶ و مجازی سازی

۶۰. Metapackage Forensic

همه ابزارهای موجود در اینجا توسط تیم ابزار امنیتی دبیان بسته بندی شده اند

ویژگی های ۶۱-۷۰

۶۱. حفاظت از ترافیک شبکه

دارای مجموعه ای از Tor، torify و ProxyChains، torsocks برای ناشناس نگه داشتن سیستم عامل

۶۲. حفاظت در برابر کشف مکان

محافظت در برابر آدرس IP، کشف مکان، موقعیت جغرافیایی، یا خدمات مکان

۶۳. MAC Address Changer

محافظت در برابر جعل آدرس MAC، یک مقدار تصادفی برای هر اتصال یا به صورت دستی توسط ابزار سفارشی ایجاد شده است..

۶۴. محافظت در برابر حمله بوت سرد

از حملات غیرفعال شدن حالت خواب زمستانی و خواب، پاک کردن حافظه، رمزگذاری تمام دیسک جلوگیری می کند.

۶۵. جلوگیری از حمله تقویت NTP

همگامسازی زمان شبکه غیرفعال است که ساعت سیستم را بین دستگاهها همگامسازی می کند تا از حمله تقویت NTP جلوگیری میکند.

۶۶. میکروکد به روز شده

به روز رسانی میکروکد CPU اعمال شد

۶۷. Password Manager Tools

دارای مدیران رمز عبور مورد اعتماد، رمزهای عبور خود را به روشی امن مدیریت میکنند

۶۸. میکروفون های غیر فعال

غیرفعال کردن میکروفون به صورت پیش فرض

۶۹. Metadata Cleaner

دارای ابزارهای حذف ابر داده

۷۰. VirtualBox Hardening

سخت شده VirtualBox

ویژگی های ۷۱-۸۰

۷۱. ACPI را غیرفعال کنید

غیرفعال کردن تنظیمات پیشرفته و رابط برق (ACPI)

۷۲. محدود کردن ماژول های هسته

محدود کردن بارگذاری ماژول می تواند از هسته محافظت کند.

۷۳. خبرنگار اشکال از کار افتاده

نرم افزار و خدمات گزارشگر اشکال غیرفعال شده است

۷۴. جلوگیری از حملات جعل جلوگیری از حملات

جعل

۷۵. کوکی های TCP/IP SYN را فعال کنید

محافظت از کوکی TCP SYN را برای ذخیره دامنه از SYN Attack فعال شده است

۷۶. ارسال بسته برای IPv۴/۷۶

به هسته اجازه می دهد تا بسته ها را از یک رابط شبکه به رابط دیگر ارسال کند

۷۷. از حملات MITM جلوگیری کنید

تغییر مسیرهای ICMP را برای جلوگیری از حملات MITM قبول نمیکند

۷۸. تغییر مسیرهای ICMP را بپذیرید

تغییر مسیرهای ICMP را فقط برای دروازه های فهرست شده در پیش فرض میپذیرد.

۷۹. اندازه کش ای نود.

افزایش اندازه دسته فایل و کش inode

۸۰. Caching و Swapping

اندازه تعویض و فشار حافظه پنهان را افزایش داده شده است.

ویژگی های ۸۱-۹۰

۸۱. نسبت کشیف

ذخیره سازی و عملکرد بهتر دیسک لینوکس

۸۲. Included گزینه امنیت شبکه

افزایش زمان SYNACK برای اتصال TCP غیرفعال

۸۳. Protect Against TCP Time-Wait

۸۴. Syncookies را کنترل شده

۸۵. Socket Send/Receive Buffer

افزایش بافر دریافت سوکت

۸۶. بافرهای حافظه را افزایش داده شد.

حداکثر خواندن/نوشتن فضای بافرهای حافظه گزینه را افزایش داده شد

۸۷. جلوگیری از حملات DOS

برای جلوگیری از حملات ساده DOS، اندازه استخر سطل‌های tcp-time-wait را افزایش داده شد.

۸۸. افزایش عدد پید

افزایش عدد pid

۸۹. IPv۶ غیرفعال

IPv۶ غیرفعال شده است

۹۰. حفاظت از جعل IP را فعال است

ویژگی های ۹۱-۱۰۰

kernel.randomize_va_space.۹۱

موقعیت های تصادفی در فضای آدرس یک فرآیند، که پیش بینی آدرس حافظه دستورالعمل بعدی را برای یک برنامه مهاجم دشوار می کند.

۹۲. تنظیم بافر TCP

محدودیت های بافر TCP تنظیم خودکار لینوکس را افزایش داده شد.

۹۳. جلوگیری از حملات Brute Force برای جلوگیری از حملات brute force، پیاده سازی نرم افزار پیشگیری از نفوذ

Fail2ban را در نظر بگیرید.

۹۴. SELinux را فعال است

۹۵. مسیریابی منبع IP را غیرفعال شد

۹۶. در برابر ترور زمان انتظار محافظت می کند

۹۷. جلوگیری از حملات مرد میانی

۹۸. اجتناب از حملات اسمورف

همه درخواست های ICMP را نادیده بگیرید تا از حملات Smurf اجتناب کنید، شمارش دستگاه در شبکه را دشوارتر کنید و از انگشت نگاری ساعت از طریق مهرهای زمانی ICMP جلوگیری میکند.

۹۹. دستگاه های بی سیم rfkill را در لیست سیاه قرار دادند تا سطح حمله از راه دور را بیشتر کاهش دهند. برای لیست سیاه همه دستگاه های بی

سیم

۱۰۰. با عملکرد بیشتر و ویژگی های تنظیم شده

contact us:

http://t.me/predator_os

<http://t.me/linuxtnt>

<https://predator-os.com/Predator-os@protonmail.com>

<https://www.instagram.com/predator.os/>

info.predator.os

<https://www.linkedin.com/in/hossein-seilany-2931891b4>

<https://github.com/hosseinseilani/>