

# Post-Installation

notes



# Predator-OS Linux<sup>V3.0</sup>

It was developed in 2021 by [Hossein Seilani](#), who is also the developer of <https://emperor-os.ir/> Linux. Predator-OS is a free and open-source community project, emphasizing freedom. The distribution is designed for penetration testing, ethical hacking, privacy, hardening, security, and anonymity. Predator Linux is based on Debian, with kernel 6.6 and 6.1 Its LTS, and utilizes a fully customized plasma desktop with a special menu of tools.

# **Predator-OS Linux** V3.0

**Penetration testing and Ethical hacking and also you can use it as:  
privacy, hardened, secure, anonymized**



# Polymorphic Security Platform

A security-centric free  
open-source Linux

# Post-Installation Notes:

- ① by default, the username and password of the predator-os:

**username: predator**

**password: predator**

- ② First, set a password for the root user:

```
$ sudo passwd root
```

- ③ **Software Compatibility**

Easily run popular applications and software packages on Predator-OS Linux thanks to its broad compatibility.

# Post-Installation Notes:

- 4 Using tools that are in Monitoring menu to control all services and start-up of applications. Please disable and stop unnecessary or enable and start necessary services with it. Some tools need its service starts, such as:

**Netdata:**

**Nessus**

**Xplic**

**Tor**

**I2p**

**And so on.**

# Post-Installation Notes:

4

Using some pre-alias commands to speed up Linux commands. Type alias command to see custom predator-os commands:

**\$alias**

Such as:

**\$up command instead of:**

**\$sudo apt update**

And more aliases:

```
alias l='ls -CF'
```

```
alias la='ls -A'
```

```
alias ll='ls -aLF'
```

```
alias ls='lsd --group-dirs first'
```

```
alias lw='librewolf'
```

```
alias off='poweroff'
```

```
alias reb='reboot'
```

```
alias sy='sudo synaptic'
```

```
alias top='htop'
```

```
alias tree='lsd --tree'
```

```
alias ug='sudo apt dist-upgrade'
```

```
alias uk='sudo update-kernel.sh'
```

```
alias up='sudo apt update'
```

```
alias wdl='wget --limit-rate=0 --tries=16'
```

# Post-Installation Notes:

**4** There are some ways to find tools:

- 1) Using App-Launcher. desktop icon that is on the left on the desktop.**
- 2) Using the whisker menu that is on the top-right corner of the desktop**



# Post-Installation Notes:

- 4 Please run the "Recommended-Tools.desktop" file located on the left side of your desktop.

This file will install a set of tools by downloading and installing them.

# Post-Installation Notes:

## ④ Using top tools Menu

It included many essential tools to easy access tools and control the system.

# Post-Installation Notes:

## ④ Recommend using the privacy Browser

I recommend using the installed Browser. Browser offers several features and enhancements that prioritize user privacy and control.

# Post-Installation Notes:

## ④ Upgrading system

For upgrading your system, please use the following command:

**\$apt dist-upgrade**

Or

**\$ug**

These commands are available to upgrade the system. I recommend using the Synaptic package manager tool to upgrade packages one by one instead of upgrading all applications at once.

# New features in version 3.0:

## ④ New Installer

Predator-OS has changed its installer from the Ubiquity installer to the Calamares installer.

# New features in version 3.0:

## ① Included the collection of bootloaders (PXE network bootloader)

syslinux is a suite of bootloaders, currently supporting DOS FAT and NTFS, filesystems (SYSLINUX), Linux ext2/ext3/ext4, btrfs, and xfs filesystems, (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-ROMs (ISOLINUX).

# New features in version 3.0:

## ① fix boot the Grub in dual boot installation

We added the :

```
GRUB_DISABLE_OS_PROBER="false"
```

Enabling os-prober allows the GRUB bootloader to detect other operating systems installed on your system. Once your system restarts, the GRUB bootloader should detect other operating systems during the boot process. They will be listed as options in the GRUB menu.

# New features in version 3.0:

## ① New Grub parameters for hardening and tuning

Included new Grub parameters for improved performance tuning and system hardening.



# New features in version 3.0:

## ① New kernel parameters for hardening and tuning

Included new kernel parameters for improved performance tuning and system hardening.

# New features in version 3.0:

- ① Fixed Grub errors while installation

# New features in version 3.0:

## ① Included secure-boot package

Secure Boot is a security feature that ensures only trusted software is loaded during the boot process, and also includes a valid digital signature recognized by the UEFI firmware.

# New features in version 3.0:

## ① Increased d-bus message bus size

Increased the maximum message size for the D-Bus session bus.

The D-Bus message bus size refers to the maximum size of messages that can be sent or received through the D-Bus system, which is a message bus system used for interprocess communication (IPC) on Linux and other operating systems.

# New features in version 3.0:

## ① Changed the password authentication configuration algorithm

Included the password hashing algorithm, password shadowing, and the 'use\_authok' option for password has changed. The password authentication configuration is set to use SHA-512 hashing.

# New features in version 3.0:

## ① Changed the password aging policies

Passwords will be expire after 30 days.

Users will need to wait at least one day before changing their passwords.

Users will be notified 7 days before their password expires.

Modified the respective lines in the `"/etc/login.defs"` file to change the password aging policies according to the specified values.

# New features in version 3.0:

## ① Changed the history length policies

The shell will only keep the last 10 commands in the history [list](#). When a new command is entered and the history exceeds the specified limit, the oldest command will be removed from the history.

The shell will only save the last 10 commands in the history [file](#). If the history file already contains more than 10 lines, the oldest commands beyond the limit will be removed from the file.

# New features in version 3.0:

## 1 New custom predator-OS alias

```
alias up='sudo apt update'  
alias uk='sudo update-kernel.sh'  
alias ug='sudo apt dist-upgrade'  
alias fix='sudo apt -f install'  
alias fm='sudo thunar'  
alias sy='sudo synaptic'  
alias reb='reboot'  
alias off='poweroff'  
alias top='htop'  
alias adl='aria2c -x16 -s16'  
alias wdl='wget --limit-rate=0 --tries=16'  
alias fx='firefox'  
alias lw='librewolf'  
alias bat='bat --theme=ansi-dark'
```



# New features in version 3.0:

## ① Disabled access time updates

Disabling access time updates on system by adding the "`noatime`" option to the `/etc/fstab` file. This option can improve performance by preventing the access timestamp of files from being updated every time they are accessed.

# New features in version 3.0:

## ① Enabled hardware acceleration

Provided a set of sections for different graphics devices. Each section specifies the device's identifier, driver, and various options related to acceleration, tear-free rendering, and Direct Rendering Infrastructure (DRI) version.

**Intel Graphics**

**Nouveau (NVIDIA open-source driver)**

**Radeon (AMD open-source driver)**

**AMDGPU (AMD proprietary driver)**

**Nvidia**

# New features in version 3.0:

## 1 Bluetooth Performance tuning

Disable Bluetooth automatic power management

Set Bluetooth HCI snoop log

Enable Bluetooth coexistence mode

Adjust Bluetooth inquiry and pagetimeout

Set Bluetooth bitrate

Disable Bluetooth automatic suspend

Set Bluetooth power output

Adjust Bluetooth idle timeout

Adjust Bluetooth inquiry and page scan type

Enable Bluetooth high-quality audio

Adjust Bluetooth link supervision timeout

Enable Bluetooth extended inquiry response

Set Bluetooth link mode

Adjust Bluetooth inquiry and page scan interval

Adjust Bluetooth inquiry and page scan window

Disable Bluetooth LE scan throttling

Set Bluetooth HCI command timeout

Configure Bluetooth EDR mode

Set Bluetooth idle period

Set Bluetooth inquiry and page scan type

# New features in version 3.0:

## ① shell performance tuning

- Enable shell command completion
- Optimize command line completion
- Disable shell bell sound
- Disable shell session logging
- Enable shell arithmetic evaluation
- Enable shell process backgrounding
- Optimize shell command line editing
- Optimize shell startup time

# New features in version 3.0:

## ① Block devices performance tuning

- Enable DMA for all devices
- Set the read-ahead buffer size
- Set the I/O scheduler to noop
- Enable log compression

# New features in version 3.0:

- 1 Disabled IRQ balancing for the Ethernet device

Disabling IRQ balancing may impact performance and load balancing

# New features in version 3.0:

## ① Included plasma performance setting

Adjust the font rendering settings

Enable subpixel hinting for font rendering

Configure font hinting style

# New features in version 3.0:

## ① Disabled all the power option plan

AllowSuspend=no

AllowHibernation=no

AllowSuspendThenHibernate=no

AllowHybridSleep=no



# New features in version 3.0:

- ① Harden network settings

# New features in version 3.0:

- ① Physical memory hardening

# New features in version 3.0:

- ① Included nekoray proxy tools

# New features in version 3.0:

- ① Configured Tor and Proxychains for anonymous browsing

# New features in version 3.0:

## ① Configured i2p Invisible Internet Project

I2P is designed to provide strong anonymity for its users. It achieves this by encrypting and routing traffic through multiple relays, making it challenging to identify the source or destination of the communication.

# New features in version 3.0:

- ① Changed the default papersize of print to A4

# New features in version 3.0:

## ① Enhanced recommended-installer tool

Updated and added new tools for recommended-installer.  
The icon of recommended-installer is on the desktop.

# New features in version 3.0:

## ① New alias to get downloading in the fastest way possible

**\$adl is a alias command for:**

```
adl='aria2c -x16 -s16'
```

**For example:**

```
adl <url>
```

**\$wdl is a alias command for:**

```
wdl='wget --limit-rate=0 --tries=16'
```

**For example:**

```
wdl <url>
```



# New features in version 3.0:

- ① New Linux Kernel version: 6.6 LTS

# New features in version 3.0:

- ① Configured Linux kernel for low latency performance

# New features in version 3.0:

## ① Increased Udev buffer

It affected the ability of udev to handle a large number of device events. Increasing the buffer size may be necessary if you have a system with a high volume of device events, such as in environments with many hot-pluggable devices.

# New features in version 3.0:

## ① Disable GPS (Global Positioning System)

### **For more anonymous and privacy**

GPS (Global Positioning System) daemon sockets refer to the communication interfaces used by GPS daemons or services to interact with GPS receivers or GPS-related software applications. These sockets allow the GPS daemon to receive data from the GPS receiver and provide location, time, and other relevant information to the client applications.

# New features in version 3.0:

## ① Disable GPS (Global Positioning System)

Disabled geolocation service and features

Disables Location-Aware Browsing

Disabled telemetry data collection

Enhanced Tracking Protection

blocked third-party cookies

# New features in version 3.0:

## 1 Disabled the automatic loading of specific kernel modules

dccp: Datagram Congestion Control Protocol

sctp: Stream Control Transmission Protocol

rds: Reliable Datagram Sockets

tipc: Transparent Inter-Process Communication

n-hdlc: Network HDLC protocol

ax25: Amateur Radio AX.25 protocol

netrom: Amateur Radio NET/ROM protocol

x25: X.25 packet-switching protocol

rose: Amateur Radio X.25 PLP (Packet Level Protocol)

decnet: DECnet networking protocol

econet: Acorn Econet protocol

af\_802154: IEEE 802.15.4 low-rate wireless personal area network protocol

ipx: IPX (Internetwork Packet Exchange) protocol

appletalk: AppleTalk networking protocol

psnap: IEEE 802.3 SNAP protocol

p8023: Unknown module (as mentioned before, it does not appear to be a standard Linux kernel module)

p8022: Unknown module (as mentioned before, it does not appear to be a standard Linux kernel module)

can: Controller Area Network protocol

atm: Asynchronous Transfer Mode protocol

# New features in version 3.0:

## 1 more features:

- 1) Added Kernel self-protection
- 2) Restricted the kernel log to the CAP\_SYSLOG capability.
- 3) Despite the value of `dmesg_restrict`, the kernel log will still be displayed in the console during boot. It restricted. These sysctls restrict eBPF to the CAP\_BPF capability and enable JIT hardening techniques, such as constant blinding.
- 5) Restricted loading TTY line disciplines to the CAP\_SYS\_MODULE capability to prevent unprivileged attackers from loading vulnerable line disciplines with the `TIOCSETD` ioctl, which has been abused in a number of exploits before.
- 6) Restricted the syscall to the CAP\_SYS\_PTRACE capability.
- 7) Disabled SysRq completely.
- 8) disabled user namespaces completely (including for root)
- 9) Restricted all usage of performance events to the CAP\_PERFMON capability
- 10) protected against time-wait assassination by dropping RST packets for sockets in the time-wait state.

# New features in version 3.0:

## 1 more features:

- 11) enable source validation of packets received from all interfaces of the machine. This protects against IP spoofing, in which an attacker sends a packet with a fraudulent IP address.
- 12) disable ICMP redirect acceptance and sending to prevent man-in-the-middle attacks and minimise information disclosure.
- 13) ignore all ICMP requests to avoid Smurf attacks, make the device more difficult to enumerate on the network and prevent clock fingerprinting through ICMP timestamps.
- 14) Source routing is a mechanism that allows users to redirect network traffic. As this can be used to perform man-in-the-middle attacks in which the traffic is redirected for nefarious purposes, the above settings disable this functionality.
- 15) Disabled TCP SACK. SACK is commonly exploited and unnecessary in many circumstances, so it should be disabled if it is not required.
- 16) Restricted usage of ptrace to only processes with the CAP\_SYS\_PTRACE capability
- 17) Prevented creating files in potentially attacker-controlled environments, such as world-writable directories, to make data spoofing attacks more difficult.
- 18) Enabled zeroing of memory during allocation and free time, which can help mitigate use-after-free vulnerabilities and erase sensitive information in memory.
- 19) Disabled slab merging, which significantly increases the difficulty of heap exploitation by preventing overwriting objects from merged caches and by making it harder to influence slab cache layout.



# New features in version 3.0:

## 1 more features:

- 20) Randomised page allocator freelists, improving security by making page allocations less predictable. This also improves performance.
- 21) Enabled Kernel Page Table Isolation, which mitigates Meltdown and prevents some KASLR bypasses.
- 22) Randomised the kernel stack offset on each syscall, which makes attacks that rely on deterministic kernel stack layout significantly more difficult,
- 23) Disabled vsyscalls, as they are obsolete and have been replaced with vDSO. vsyscalls are also at fixed addresses in memory, making them a potential target for ROP attacks.
- 24) Disabled debugfs, which exposes a lot of sensitive information about the kernel.
- 25) Prevented information leaks during boot
- 26) Disabled the entire IPv6 stack which may not be required if you have not migrated to it. Do not use this boot parameter if you are using IPv6.

# New features in version 3.0:

## ① more features:

- 27) Increased the number of hashing rounds for passwd
- 28) Randomised the MAC address upon each boot
- 29) TCP timestamps is /disabled
- 30) Core dumps is disabled
- 31) Microcode updated
- 32) Added the IOMMU in grub boot menu

# Support and contact

## Telegram

@seilany

## GitHub

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

## Youtube

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

## Email

info.emperor-os@gmail.com

## Linkedin

<https://www.linkedin.com/in/hossein-seilani>

## All about me

<https://seilany.ir/>