WHAT is Predator-OS?

The OS that naturally preys on others

It is maintained and Established in 2021, by **Hossein Seilany** who is also the developer of Emperor-os Linux too. Predator-OS is a free open-source community project, Free (as in freedom). The distro is for penetration testing and ethical hacking and also privacy, hardened, secure, anonymized Linux. Predator Linux is based on Ubuntu 20.04 LTS Mini, kernel 5.10 LTS, and using a fully customized xfce4 lightweight desktop with a special menu of tools. Predator Linux has around 1300 pre-installed tools which are split into 40 several categories. Predator Tools are imported from both Debian and Ubuntu repositories and GitHub page. Most kernel and user configs are customized by default to prevent any hacking, non-privileged access and reduce the attack surface. many built-in firewalls and defensive tools allow end-users to control the Predator-OS. Predator also supports much privacy, anonymized, security tools, and also both it to be run as Live-CD or from a USB Drive and installation mode.

All 100 features of the predator-OS:

1.security-oriented Linux distribution

2.Xfce as the default desktop environment

3.Operates at 9 several differnt modes

4.Update Manager Tools

kernel and tools update manager, Update notifications can notify the user if their system is becoming out of date

5.collection of security tools

Predator Linux has around 1300 pre-installed tools which are split into 40 categories

6.Graphical boot system and logger

OS has a plymouth and you can press arrow key to see the console message

7.Live Mode by default, Live DVD Live USB

Also, you can run the installer and install it

8.XFce-Panel

Application launchers, menus, a workspace switcher and more plugins

9.Ulauncher

It very easy to find and launch your files, quickly open websites, find programs to open, calculate math problems, and more

10.Customized Menu

Os Allows easy and fast access to all pre-installed app, splitted into 40 categories

Features 11-20

11.Terminal in Desktop Background

highly configurable Graphics, always be open and running in desktop background

12.disabled suspend, Hibernate, sleep

Because of prevent access to the entire memory dump and private data, passwords, keys

security threat

13.Privacy Tools

PrivacyTools provides services, tools and knowledge to protect your privacy against global mass surveillance.

14.fully OSINT Framword

Focused on gathering information from free tools or resources

15.Bug Bounty Tools

Give users the ability to harness a large group of hackers in order to find bugs in their code.

16.Included Cyber Search Engine

Private Search Engines with popular features and latest links

17.CTF Tools

Running a capture, the flag (CTF) competition, Tools used for solving CTF challenges

18.Penetration Testing Lab

There are many tools to learn the practical side of vulnerability assessments and virtual space to test malware

19.Most Scaner Drivers

More than 2500 scaner devices supported by sane package

20.Privacy-enhanced browsers

privacy focused browser, shields FOR privacy, Blocking harmful ads

Features 21-30

21.Secure Group Chat Tools

included secure messaging app. End-to-end encryption, multi-mode messaging, Multi-platform support

22.self-destruct Tool

Clean Every Logs, tracks, memory, cache and fast Shutdown PC

security threat

23.VPN Tools

secure all data communications and extend private network.securely access corporate network through an encrypted connection

24.Smart and user-friendly SHELL

Included zsh and fish shell

25.Included IDS/IPS Tools

Antivirus, Trojan Remover, malware Detection, apparmore, AIDE, SElinux and Firewalls

26.Integrity Check Tools

Included tools to compare state of stored data and file integrity monitoring

27.Apparmor Profiles

Installed and enabled all available apparmor profiles

28.Included USB Guard Tools

Prevent from USB, physical access and Electrical attacks

29.Included Tune utility

The tuned command-line tool allows users to switch between different tuning profiles.

30.Real time monitoring Tool

Monitoring and troubleshooting everything in real time for free with Netdata

Features 31-40

31.Google Hacking Database

You can access to more than 6 entries

32.controlling All services

included Stacer tool to controlling all services beside the systemctl cli

33.Removing Unnecessary data

Removing Unnecessary services, packages, startup files and configs

34.disabled the [Ctrl]-[Alt]-[Delete]

Disallow anyone to reboot the OS using Ctrl-Alt-Del keys.

35.Included Database Tools

included the most useful database management tools

36.Included Audit Tools

Included Security Audit and Intrusion Detection Tool: tiger, lynis and more tools

37.included Mix Networks protocols

Hard-to-trace communications, by encrypting and keep you anonymous online.such as i2p,Tor,OpenVPN,Lantern

38.Included osquery

Allows you to craft your system queries using SQL statements to troubleshoot performance and operational issues

39.Included log management tools

Managing and analyzing log files, record system activity, events and report generation tools

40.password lists

Access to 300 GB password list contains every wordlist, dictionary, and password database leak

Features 41-50

41.included wipe tools

fully erase data from hard drive, memory, rewrites the sector and flushes the cache

42.Included Virtual Keyboard

Florence is an open source extensible scalable virtual keyboard

43.Malware Analysis Toolkit

included Toolkit for reverse-engineering and analyzing Windows and Linux malicious, Forensic investigators

44.Machine Learning for Cybersecurity

included python2 and 3 modules for InfoSec, malware analysis, cyber security and Machine Learning

45.Self-document of tools

Describes the application with extra lines as a tools tooltip.

46. package managers

Included apt, aptitude, alien, synaptic, dpkg, snap

47.Kernel tuning

included Kernel tuning configurations such as high cache pressure, tuned performance profile

48.Included cpupower Tools

Included collection of tools to examine and tune power saving related features of your processor.

49.Data Recovery Tools

Included Tools for lose data, critical information either through accidental deletion, virus attacks, corrupted data permanent removal of files

50.Forensic Metapackage

All here available tools are packaged by Debian Security Tools Team

Features 51-60

51.included Sleuth Kit

collection of command line tools to analyze disk images and recover files from them

52.ExecShield Buffer Overflows

Protecting against buffer overflows

53.Securing network access

Protected against syn packet flooding and ARP attacks

54.Disabled Auto-mounting

Turn off removable drives Auto-mounting feature

55.Disabled virtual machine shared folders

Disabled Mounting virtual machine shared folders between host and guest

56.Normal user as defualt

Used normal user as defualt, consider disabling the root account permanently and run the command with sudo

57.Volume or container encryption

Included symmetric and asymmetric encryption tools for files and volumes

58.Included ASLR

Address Space Layout Randomization.all randomization prevent the exploitation of memory corruption vulnerabilities

59.x86 compatible and Virtual Machines

Supported x86 compatible and Virtual Machines and virtualization

60.Forensic Metapackage

All here available tools are packaged by Debian Security Tools Team

Features 61-70

61.Protecting Network Traffic

Included a collection of Tor, torify, and torsocks, ProxyChains to keeping OS anonymized

62.Protection against location discovery

Protection against IP address, location discovery,Geolocation, or location services

63.MAC address Changer

Protected against spoofing of the MAC address, generate a random value for each connection or manually by custom tool

64.Cold boot attack protection

Prevents attacks by disabled hibernation and sleep modes, wipe memory, full-disk encryption

65.Prevent NTP amplification attack

Disabled Network time synchronization which synchronize system clock between devices to prevent NTP amplification attack.

66.Updated Microcode

Applied CPU microcode updates

67.Password Manager Tools

Included Trusted password managers,manage your passwords in a secure way

68.Disabled Microphones

Disabling Microphones by default

69.Metadata Cleaner

Included Metadata Removal Tools

70.VirtualBox Hardening

VirtualBox Hardening

Features 71-80

71.Disable ACPI

Disable Advanced Configuration and Power Interface (ACPI)

72.Restricting kernel modules

Restricting module loading can protect the kernel.

73.Disabled bug reporter

Disabled bug reporter software and services

74.preventing spoofing attacks

preventing spoofing attacks

75.Enable TCP/IP SYN cookies

Enable TCP SYN cookie protection to save domain from SYN Attack

76.Packet forwarding for IPv4/v6

Permits the kernel to forward packets from one network interface to another

77.Prevent MITM Attacks

Do not accept ICMP redirects to prevent MITM attacks

78.Accept ICMP redirects

Accept ICMP redirects only for gateways listed in our default

79.Size of inode cache

Increase size of file handles and inode cache

80.Swapping and Caching

Increase size of swappiness and cache pressure

Features 81-90

81.Dirty Rratio

Better Linux Disk Caching & Performance

82.Included Network security option

Increasing times SYNACKs for passive TCP connection

83.Protect Against TCP Time-Wait

84.Control Syncookies

85.Socket Send/Receive Buffer

Increasing Socket Receive Buffer

86.Increase memory buffers

Increase the maximum read/write of option memory buffers space

87.Prevent DOS attacks

Increase the tcp-time-wait buckets pool size to prevent simple DOS attacks

88.Increasing pid number

Increasing pid number

89.Disabled IPv6

Disabled IPv6

90.Enable IP spoofing protection

Enable IP spoofing protection

Features 91-100

91.kernel.randomize_va_space

Random positions in a process's address space, which makes it difficult for an attacking program to predict the memory address of the next instruction

92. Tuning TCP buffer

Increase Linux auto tuning TCP buffer limits

93.Prevent Brute force attacks

preventing brute force attacks, consider implementing the intrusion prevention software Fail2ban

94.Enabled SELinux

95.Disable IP source routing

96.protects against time-wait assassination

97.prevent man-in-the-middle attacks

98.avoid Smurf attacks

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.

99.Wireless devices blacklisted

rfkill to reduce remote attack surface further. To blacklist all wireless devices

100.Grsecurity