

Mengintip Jurang: Panduan Dark Web yang Seharusnya Tidak Anda Perlukan

Onno W. Purbo
onno@indo.net.id
onno@itts.ac.id
Twitter onnowpurbo

**Institut Teknologi Tangerang Selatan
2025**

Lisensi

Buku ini dilisensikan di bawah **Creative Commons Attribution 4.0 International License (CC BY 4.0)**.

Anda bebas untuk:

- **Berbagi** — menyalin dan menyebarkan materi ini dalam bentuk dan media apa pun.
- **Mengadaptasi** — mengubah, mengubah, dan membuat turunan dari materi ini untuk tujuan apa pun, termasuk tujuan komersial.



Dengan ketentuan:

- **Atribusi** — Anda harus memberikan kredit yang sesuai kepada penulis (*Onno W. Purbo*), menyertakan tautan lisensi, dan menunjukkan jika ada perubahan yang dilakukan. Anda dapat melakukannya dengan cara yang wajar, namun tidak dengan cara yang menyiratkan bahwa pemberi lisensi mendukung Anda atau penggunaan Anda.

Lisensi lengkap dapat dilihat di:

<https://creativecommons.org/licenses/by/4.0/>

© 2025 Onno W. Purbo.

Daftar Isi

Lisensi.....	2
Daftar Isi.....	3
Kata Pengantar.....	5
BAB: Konsep Dasar Dark Web.....	7
Peringatan Penting 	7
Surface Web (Web Permukaan).....	8
Deep Web (Web Dalam).....	8
Dark Web (Web Gelap).....	9
Ringkasan dalam Tabel.....	9
Highlights.....	10
Kenapa Perlu Dipahami?.....	10
BAB: Legalitas dan Resiko Dark Web.....	11
Point Penjelasan.....	11
Penjelasan dalam Tabel.....	11
Resiko Akses Dark Web.....	12
Risiko Keamanan.....	12
Risiko Hukum.....	12
Ringkasan Risiko dalam Tabel.....	13
Tips Mitigasi (Jika untuk Tujuan Legal & Penelitian).....	13
BAB: Konsep Dasar Anonimitas di Tor.....	14
Faktor yang Dapat Membocorkan Identitas.....	14
Diagram Alur kebocoran Identitas di Tor.....	14
Perbandingan: Anonimitas Ideal vs Risiko Nyata.....	15
Langkah Pencegahan.....	15
BAB: Persiapan Masuk ke Dark Web di Kali Linux.....	16
Persiapan Sistem.....	16
Instalasi Tor Browser.....	16
Menjalankan Tor Browser.....	16
Siap Menjelajah.....	17
BAB: Akses Situs Dark Web.....	18
4. Akses Situs Dark Web.....	18
5. Mencari Informasi di Dark Web.....	18
6. Tips Keamanan Tambahan.....	18
Langkah 3: Memahami Alamat .onion dan Mencari Informasi.....	19
Mesin Pencari Populer di Dark Web:.....	19
Cara Praktis Mencari Informasi:.....	19
BAB: DarkRadar.io.....	21
Fitur Utama DarkRadar.io.....	21
Keunggulan DarkRadar.io.....	22
Konteks CyberArmyID.....	22
Manfaat untuk Pengguna.....	22
Cara Menggunakan DarkRadar.io.....	22

Kesimpulan.....	23
Praktek Menggunakan DarkRadar.....	23
BAB: Praktik Terbaik untuk Keamanan dan Anonimitas di Dark Web.....	30
Referensi.....	32
Tentang Penulis.....	33

Kata Pengantar

BAB: Konsep Dasar Dark Web

Dark web adalah bagian dari deep web yang tidak terindeks oleh mesin pencari konvensional dan biasanya diakses melalui jaringan anonim seperti Tor. Mengakses dark web legal selama Anda tidak terlibat dalam aktivitas ilegal, tetapi ini berisiko karena potensi malware, penipuan, dan konten ilegal. Selalu prioritaskan keamanan: gunakan VPN sebelum Tor untuk lapisan anonimitas ekstra, jangan bagikan data pribadi, hindari unduh file mencurigakan, dan gunakan antivirus. Panduan ini berfokus pada Kali Linux, yang sudah mendukung alat keamanan.

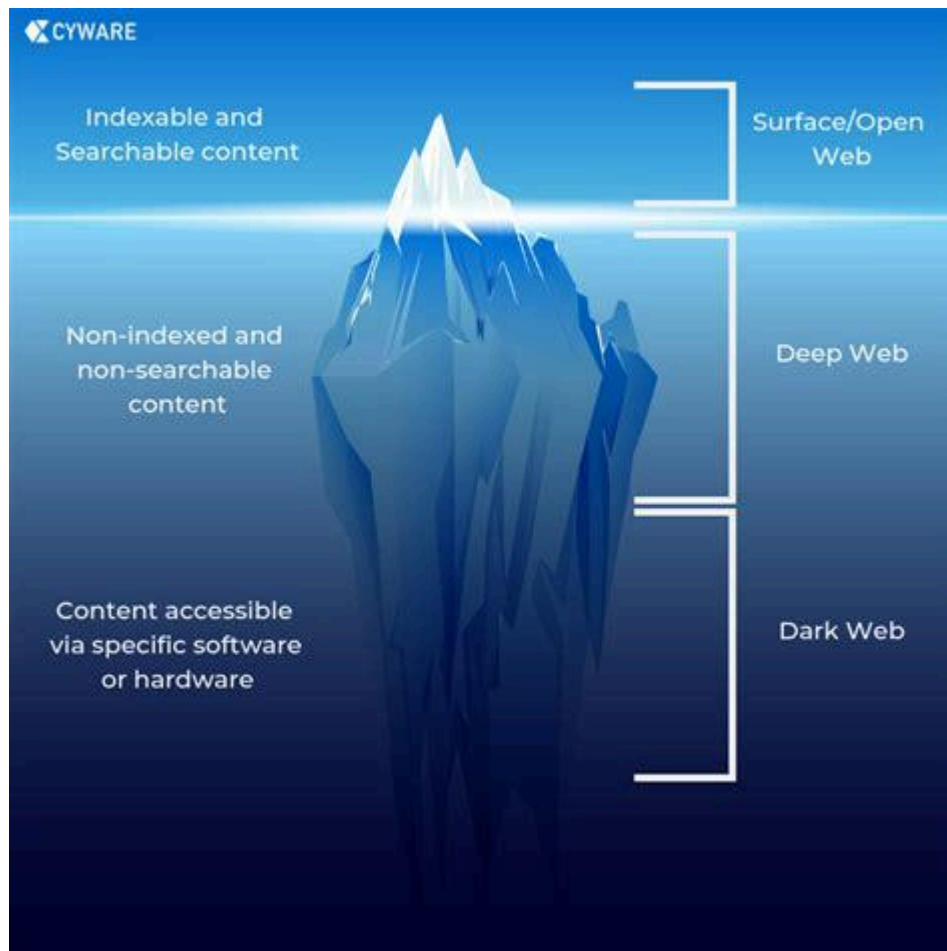
Catatan Penting: Saya bukan penasihat hukum; pastikan aktivitas Anda sesuai undang-undang di negara Anda. Gunakan dark web hanya untuk tujuan edukasi atau penelitian etis.

Peringatan Penting

Sebelum melanjutkan, pahami risiko-risiko berikut:

- **Keamanan:** *Dark web* berisi banyak konten ilegal dan berbahaya, termasuk *malware*, situs penipuan (*phishing*), dan materi ekstrem.
- **Legalitas:** Mengakses beberapa bagian dari *dark web* atau mengunduh konten tertentu dapat melanggar hukum di negara Anda. Anda bertanggung jawab penuh atas tindakan Anda.
- **Anonimitas:** Meskipun Tor dirancang untuk anonimitas, kesalahan konfigurasi atau tindakan ceroboh dapat membocorkan identitas Anda.

Gunakan informasi ini untuk tujuan pendidikan dan penelitian yang sah. **Jangan pernah terlibat dalam aktivitas ilegal.**



Berikut diagram *iceberg* yang menggambarkan tiga lapisan utama internet: **Surface Web**, **Deep Web**, dan **Dark Web**.

Surface Web (Web Permukaan)

Surface Web—juga dikenal sebagai *visible*, *indexed*, atau *clearnet*—adalah bagian internet yang **mudah diakses** lewat *search engines* seperti Google, Bing, atau Yahoo. Cukup dengan browser biasa (Chrome, Firefox, dan sejenisnya), siapa saja dapat menemukannya tanpa konfigurasi khusus ([CIS](#)).

- Contoh: situs berita, media sosial, e-commerce, blog publik seperti Wikipedia ([insightindia.com](#)).
- Mencakup hanya **sekitar 10 %** dari seluruh konten internet ([Wikipedia](#)).

Deep Web (Web Dalam)

Deep Web mencakup segala konten yang **tidak terindeks oleh search engine**. Ini termasuk halaman yang hanya bisa diakses lewat login, URL langsung, atau melalui intranet dan database internal ([CIS](#), [Wikipedia](#), [Check Point Software](#)).

- Contoh: akun email, perbankan online, dokumen pemerintah, media bayar (*paywall*), sistem akademik, layanan cloud ([KnowBe4 Blog](#)).

- Merupakan bagian terbesar internet — diperkirakan **90–95 %** dari total konten berada di sini ([Check Point Software](#)) (“400–550 kali lebih besar” daripada Surface Web) ([WIRED](#)).

Dark Web (Web Gelap)

Dark Web adalah subset dari Deep Web, namun dengan akses yang jauh lebih terbatas. Pengguna memerlukan **perangkat lunak khusus** (seperti *Tor*, *I2P*) dan alamat unik (sering berakhiran *.onion*) untuk masuk ([CIS](#), [Wikipedia](#), [Fortinet](#)).

- Dirancang untuk menjamin **anonimitas tinggi** bagi pengguna dan host ([Wikipedia](#), [Investopedia](#)).
- Walau terkenal karena aktivitas ilegal (pasar gelap, malware, penjualan data curian), *Dark Web* juga digunakan untuk tujuan sah seperti komunikasi aman bagi jurnalis, pelapor (whistleblower), atau aktivis di rezim otoriter ([Investopedia](#)).
- Proporsi relatif kecil: kurang dari **0,01 %** dari keseluruhan internet, dengan sekitar **10.000 layanan tersembunyi Tor** ([WIRED](#)).

Ringkasan dalam Tabel

Lapisan Web	Akses & Browser	Konten Contoh	Rasio/peran
Surface Web	Terindeks, diakses oleh browser umum	Situs publik: berita, media sosial, e-commerce	~10 % informasi internet (Wikipedia)
Deep Web	Tidak terindeks, perlu kredensial atau URL	Akun pribadi, sistem internal, paywall, database	~90–95 % konten internet (Check Point Software , WIRED)
Dark Web	Butuh Tor/I2P, alamat khusus (.onion)	Pasar gelap, whistleblower, aktivisme rahasia	< 0,01 % internet, sekitar 10 k layanan (WIRED)

Highlights

- **Surface Web** adalah bagian internet yang *terindeks* dan mudah diakses.
- **Deep Web** merupakan area **private & terlindungi** (login/password, paywall, dsb.), dan sangat besar.
- **Dark Web** adalah sub-lapisan yang **super-rahasia**, menggunakan *overlay networks* seperti Tor untuk **anonimitas**, digunakan untuk **aktivitas ilegal sekaligus komunikasi aman**.
- Meski jumlahnya kecil, *Dark Web* sering **salah disamakan** dengan Deep Web—padahal fungsinya berbeda ([Wikipedia](#), [Wikipedia](#)).

Kenapa Perlu Dipahami?

- Untuk memahami **risiko keamanan digital**: misconfigurations bisa mengekspos data dari Deep Web ke Surface Web, menyebabkan pelanggaran data ([CIS](#)).
- Untuk **membedakan penggunaan**: Deep Web mayoritas digunakan untuk hal sah sehari-hari, sedangkan Dark Web punya dualitas—aktivitas **ilegal sekaligus perlindungan terhadap pengawasan** ([YouTube](#)).
- Untuk **kesadaran privasi** dan potensi eksploitasi data: meskipun tidak ilegal mengakses Dark Web, bisa berbahaya tanpa langkah keamanan seperti VPN atau browser Tor ([Check Point Software](#)).

Secara garis besar, internet bukan cuma *apa yang terlihat oleh Google*. Mengetahui **Surface Web**, **Deep Web**, dan **Dark Web** membantu kita navigasi dan pahami dunia maya secara lebih bijak dan aman.

BAB: Legalitas dan Resiko Dark Web

Mengakses *dark web* tidak selalu ilegal, karena ada bagian yang digunakan untuk tujuan sah seperti komunikasi aman atau perlindungan privasi. Namun, beberapa bagian *dark web* digunakan untuk kegiatan terlarang seperti perdagangan narkoba, senjata, data pribadi curian, atau materi yang melanggar hak cipta. Mengunduh atau mengakses konten tersebut dapat melanggar hukum di banyak negara, termasuk undang-undang pidana, hak cipta, dan perlindungan data. Pelanggaran ini bisa mengakibatkan sanksi berat, seperti denda besar atau hukuman penjara. Oleh karena itu, sangat penting memahami hukum yang berlaku di negara Anda sebelum mengakses konten *dark web*.

Point Penjelasan

- **Tidak semua *dark web* ilegal:** Ada situs yang digunakan untuk kebebasan pers, komunikasi anonim, atau perlindungan privasi.
- **Risiko hukum tinggi** jika mengakses:
 - Pasar gelap (*black market*).
 - Konten pornografi ilegal.
 - Data pribadi yang dicuri.
 - Barang atau jasa terlarang.
- **Undang-undang yang mungkin dilanggar:**
 - UU ITE (di Indonesia).
 - Undang-undang anti-terorisme.
 - Peraturan hak cipta.
 - UU perlindungan data pribadi.
- **Sanksi:** Denda besar, hukuman penjara, atau keduanya.
- **Tips aman:** Gunakan untuk tujuan sah, hindari mengunduh file dari sumber tak dikenal, dan pahami regulasi hukum lokal.

Penjelasan dalam Tabel

Aspek	Penjelasan	Contoh Aktivitas Ilegal	Potensi Sanksi
Akses Konten	Mengunjungi situs dark web tertentu yang berisi konten ilegal	Mengunjungi pasar narkoba online	Hukuman penjara, denda
Unduhan Data	Mengambil file dari sumber terlarang di dark web	Mengunduh database kartu kredit curian	Denda besar, penjara
Penyebaran	Membagikan atau menjual kembali konten ilegal	Menjual data pribadi orang lain	Penjara, sanksi perdata dan pidana
Perantara	Membantu orang lain mengakses atau membeli barang/jasa ilegal di dark web	Menjadi kurir digital untuk penjualan senjata	Hukuman berat sesuai peran dalam kejahatan

Kepemilikan	Memiliki file ilegal, meski tidak digunakan	Menyimpan materi pornografi anak	Penjara jangka panjang, denda maksimum
--------------------	---	----------------------------------	--

Resiko Akses Dark Web

Akses ke **dark web** membawa risiko yang signifikan, baik dari sisi keamanan digital maupun hukum. Walaupun dark web digunakan untuk berbagai tujuan (termasuk yang legal), bagian besar dari aktivitas di sana terkait dengan aktivitas ilegal yang melibatkan malware, penipuan, dan kejahatan dunia maya. Berikut penjelasan dalam format campuran paragraf, poin, dan tabel.

Risiko Keamanan

Mengakses dark web berarti terpapar pada lingkungan yang tidak diatur dan minim pengawasan. Beberapa ancaman yang sering ditemui:

- **Malware:** File atau tautan yang terlihat biasa dapat mengandung ransomware, keylogger, atau trojan yang mencuri data.
- **Phishing:** Situs yang meniru layanan terkenal untuk mencuri kredensial pengguna.
- **Penipuan:** Penjual fiktif yang menawarkan barang atau jasa namun menghilang setelah pembayaran.

Risiko Hukum

- **Kepemilikan atau distribusi konten ilegal** (misalnya materi eksploitasi anak, data curian, atau narkoba) dapat menimbulkan tuntutan pidana.
- **Undang-undang nasional** di banyak negara memiliki pasal yang tegas terkait aktivitas di dark web, termasuk sekadar mengakses situs tertentu.
- **Pengawasan aparat:** Beberapa marketplace atau forum di dark web diamati oleh badan penegak hukum untuk melacak pelaku kejahatan.

AKSES KE DARK WEB

RISIKO & KEAMANAN

Risiko Keamanan

Malware

Phishing

Penipuan

Risiko Hukum

- Kepemilikan atau distribusi konten ilegal
- Undang-undang nasional
- Pengawasan aparat

Ringkasan Risiko

Malware
Program berbahaya

Phishing
Mencuri data

Penipuan
Transaksi palsu

Risiko hukum
Tuntutan pidana

Ringkasan Risiko dalam Tabel

Risiko	Deskripsi	Dampak Potensial	Contoh Kasus
Malware	Program berbahaya yang menyusup ke perangkat lewat unduhan atau tautan	Kehilangan data, kerusakan sistem, pencurian identitas	Ransomware mengunci file pengguna
Phishing	Penipuan yang menyamar sebagai situs/layanan terpercaya untuk mencuri data	Kebocoran akun, kehilangan akses layanan	Login palsu meniru dompet kripto
Penipuan	Transaksi fiktif tanpa pengiriman barang/jasa	Kehilangan uang	Marketplace palsu di dark web
Risiko hukum	Aktivitas ilegal atau akses konten terlarang yang dapat menyalahi hukum nasional	Tuntutan pidana, denda, penjara	Pembelian data curian atau narkoba online

Tips Mitigasi (Jika untuk Tujuan Legal & Penelitian)

- Gunakan **sistem operasi live** (mis. Tails OS) yang tidak menyimpan jejak.
- Lindungi identitas dengan **VPN + Tor** (layer ganda).
- Hindari login ke akun pribadi atau mengunduh file dari sumber yang tidak jelas.
- Pastikan memahami **hukum setempat** sebelum mengakses konten atau layanan.

BAB: Konsep Dasar Anonimitas di Tor

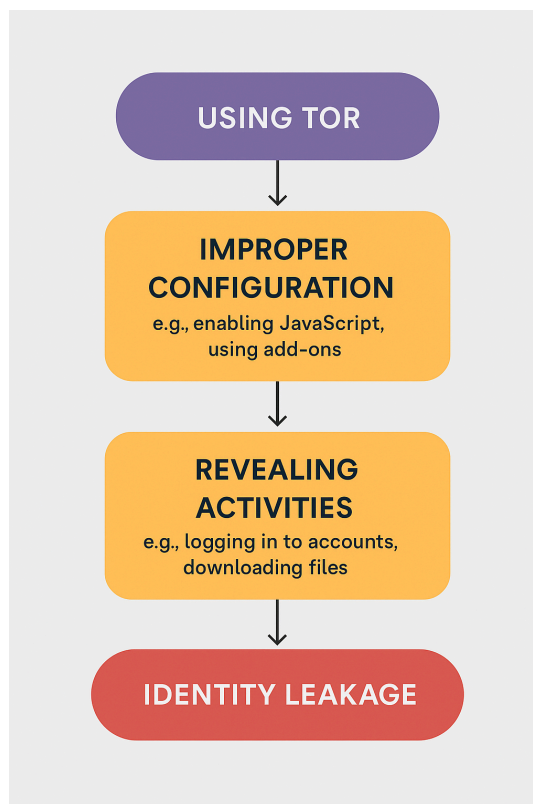
Tor (The Onion Router) dirancang untuk menyembunyikan identitas dan lokasi pengguna dengan memantulkan lalu lintas internet melalui jaringan relawan yang terdistribusi. Setiap lapisan enkripsi bekerja seperti “kulit bawang” untuk mempersulit pihak ketiga melacak sumber koneksi. Namun, **anonimitas ini tidak absolut** — kesalahan teknis maupun perilaku dapat mengungkap identitas asli.

Faktor yang Dapat Membocorkan Identitas

Beberapa hal yang sering menjadi penyebab kebocoran identitas saat menggunakan Tor antara lain:

- **Kesalahan konfigurasi browser** – Misalnya mengaktifkan JavaScript pada situs yang tidak aman.
- **Penggunaan plugin/add-ons** – Beberapa ekstensi dapat melewati jalur Tor dan mengirimkan alamat IP asli.
- **Login ke akun pribadi** – Mengakses email, media sosial, atau layanan lain yang terhubung dengan identitas asli.
- **Mengunduh file langsung** – File yang diunduh (terutama PDF, DOCX) bisa memuat skrip yang mengirim data ke luar Tor.
- **Menggunakan protokol non-HTTP/HTTPS tanpa perlindungan tambahan** – Seperti FTP yang tidak terenkripsi.

Diagram Alur kebocoran Identitas di Tor



Perbandingan: Anonimitas Ideal vs Risiko Nyata

Aspek	Kondisi Ideal (Tor Berfungsi Penuh)	Risiko Nyata Akibat Kesalahan
Alamat IP	IP asli sepenuhnya tersembunyi	IP asli dapat terekspos lewat kebocoran DNS/WebRTC
Lokasi	Tidak dapat dilacak	Bisa terlacak jika mengakses layanan berbasis lokasi
Identitas	Tidak terkait dengan aktivitas	Terkait langsung jika login ke akun pribadi
Riwayat Aktivitas	Tersebar di banyak node sehingga sulit dianalisis	Dapat dikaitkan jika menggunakan fingerprinting browser

Langkah Pencegahan

- Gunakan **Tor Browser resmi** tanpa modifikasi.
- Nonaktifkan JavaScript untuk situs yang tidak dipercaya.
- Jangan login ke akun yang menggunakan identitas asli.
- Gunakan VPN tambahan sebelum mengakses Tor (double protection).
- Hindari mengunduh atau membuka file langsung dari Tor tanpa memutuskan koneksi internet terlebih dahulu.

BAB: Persiapan Masuk ke Dark Web di Kali Linux

Persiapan Sistem

Sebelum memulai, pastikan Kali Linux Anda berada dalam kondisi terbaru. Buka terminal, lalu jalankan perintah:

```
sudo apt update && sudo apt upgrade -y
```

Langkah ini akan memperbarui semua paket ke versi terkini. Untuk keamanan tambahan, disarankan menggunakan VPN seperti OpenVPN atau ProtonVPN yang dapat diinstal melalui repository Kali. Aktifkan VPN sebelum melanjutkan agar koneksi Anda lebih terlindungi.

Instalasi Tor Browser

Tor Browser adalah alat utama untuk mengakses dark web, karena dapat menyamarkan identitas Anda dengan merutekan lalu lintas internet melalui jaringan server sukarelawan (node) di seluruh dunia.

Pada Kali Linux, tidak disarankan menjalankan Tor Browser sebagai *root user*. Jika Anda belum memiliki akun pengguna standar, buatlah terlebih dahulu untuk alasan keamanan.

Buka terminal, kemudian jalankan perintah berikut untuk menginstal Tor dan Tor Browser Launcher:

```
sudo apt install -y tor torbrowser-launcher
```

Paket ini akan mengunduh, memverifikasi tanda tangan digital, dan memasang Tor Browser secara otomatis jika belum ada di sistem Anda.

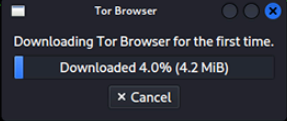
Menjalankan Tor Browser

Setelah instalasi selesai, jalankan Tor Browser menggunakan perintah:

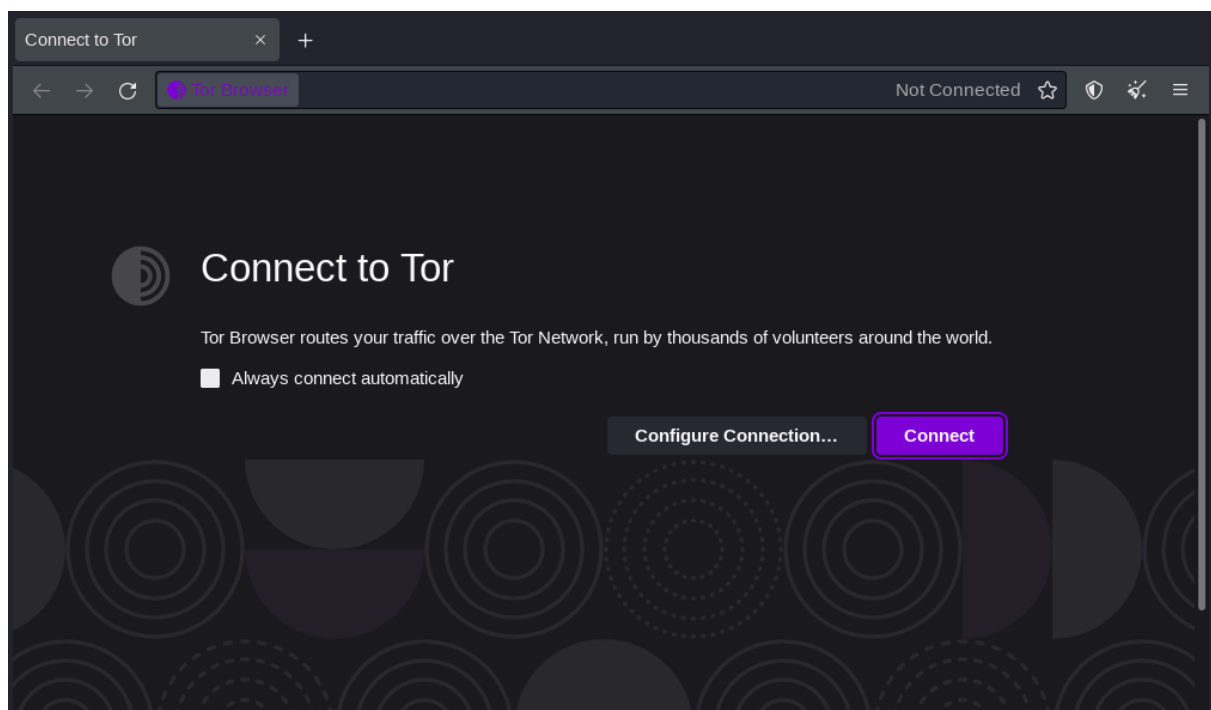
```
torbrowser-launcher
```

Perintah ini harus dijalankan sebagai pengguna biasa, bukan root. Pada penggunaan pertama, sistem akan mengunduh file Tor Browser sekaligus melakukan verifikasi. Proses ini bisa memakan waktu beberapa menit.

```
user90@desk:~$ torbrowser-launcher
Tor Browser Launcher
By Micah Lee, licensed under MIT
version 0.3.5
https://github.com/micahflee/torbrowser-launcher
Downloading Tor Browser for the first time.
Downloading https://aus1.torproject.org/torbrowser/update_3/release/Linux_x86_64-gcc3/x/en-US
Latest version: 11.5
Downloading https://dist.torproject.org/torbrowser/11.5/tor-browser-linux64-11.5_en-US.tar.xz.asc
Downloading https://dist.torproject.org/torbrowser/11.5/tor-browser-linux64-11.5_en-US.tar.xz
```

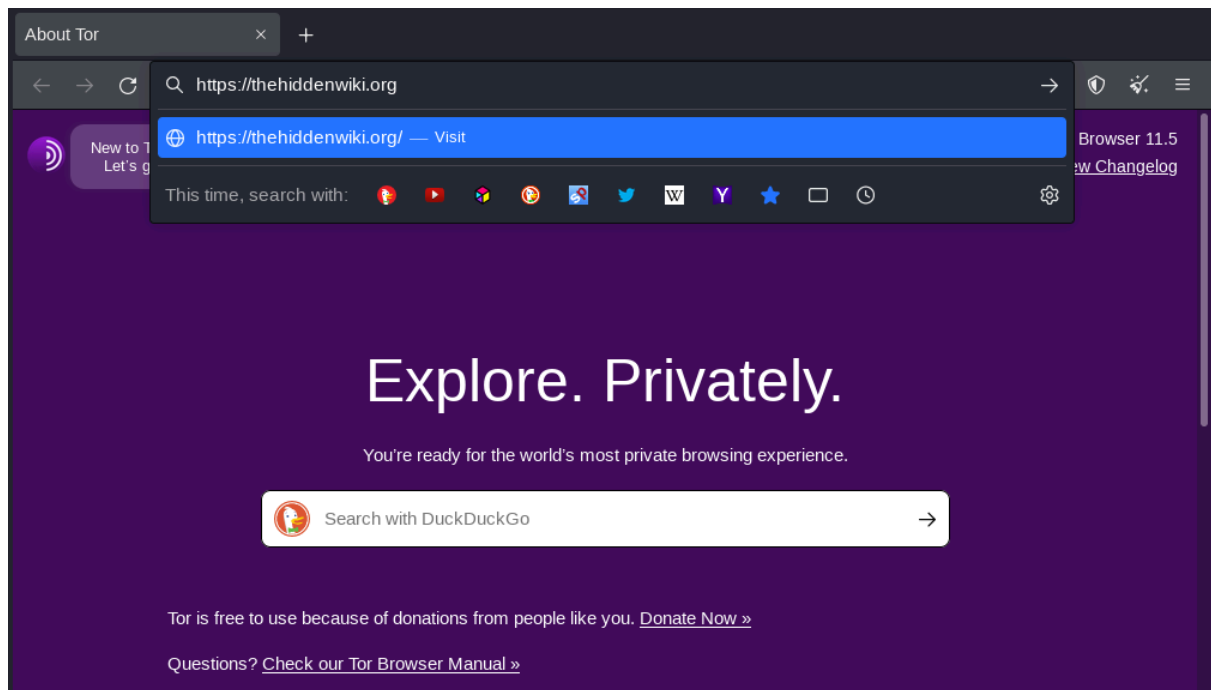
A small window titled "Tor Browser" showing a progress bar for downloading the Tor Browser. The text inside says "Downloading Tor Browser for the first time." and "Downloaded 4.0% (4.2 MiB)". There is a "Cancel" button at the bottom.

Begitu jendela Tor Browser terbuka, Anda akan melihat opsi **Connect** untuk langsung terhubung ke jaringan Tor. Klik opsi ini jika Anda berada di wilayah tanpa pembatasan internet yang ketat. Namun, jika Anda berada di negara atau jaringan dengan firewall ketat (misalnya Tiongkok atau Iran), pilih **Configure** untuk mengatur *bridges* atau *pluggable transports*.



Siap Menjelajah

Setelah koneksi berhasil dibuat, Tor Browser akan menampilkan jendela utama yang mirip dengan Firefox (karena memang dibangun di atasnya). Semua koneksi Anda kini dirutekan melalui jaringan Tor, menjaga anonimitas dan keamanan. Disarankan untuk tidak mengubah pengaturan default agar perlindungan tetap optimal.



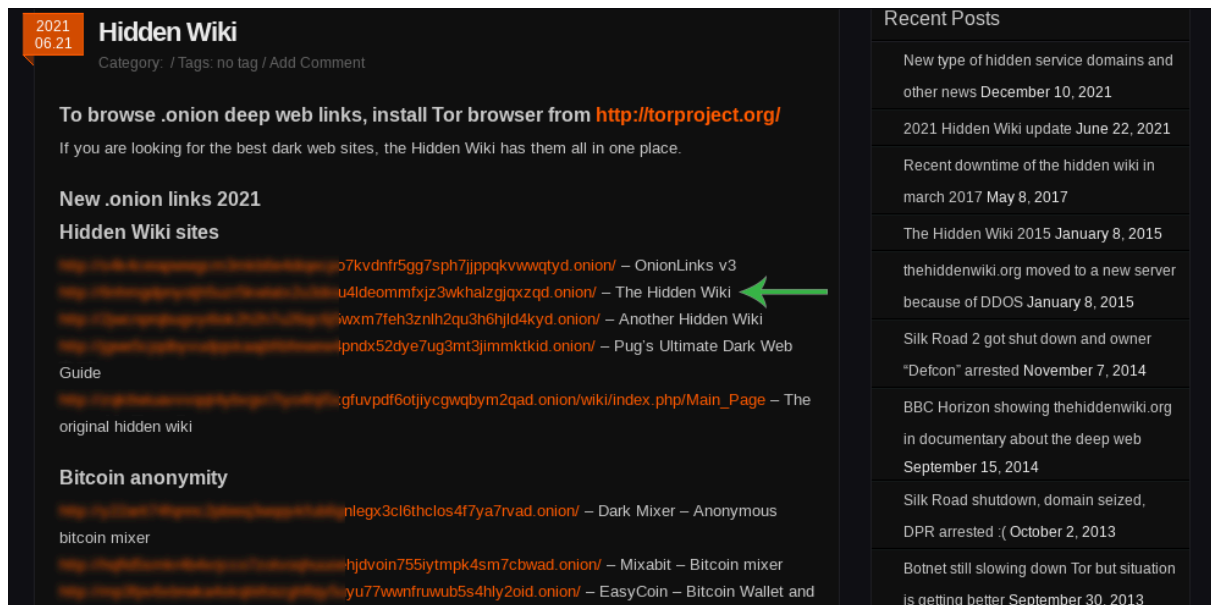
Tangkapan layar ini menunjukkan jendela **Tor Browser** yang telah berhasil terkoneksi ke jaringan Tor. Pada bagian tengah layar terdapat pesan "*Explore. Privately.*" yang menandakan bahwa pengguna sudah siap menjelajah internet secara pribadi dan aman. Tor Browser di sini menggunakan **DuckDuckGo** sebagai mesin pencari default, memberikan perlindungan privasi tambahan saat berselancar di dunia maya.

Di bagian atas, terlihat bilah alamat yang sedang mengarah ke situs <https://thehiddenwiki.org/>, salah satu direktori terkenal yang memuat tautan menuju berbagai layanan di dark web.

Catatan:

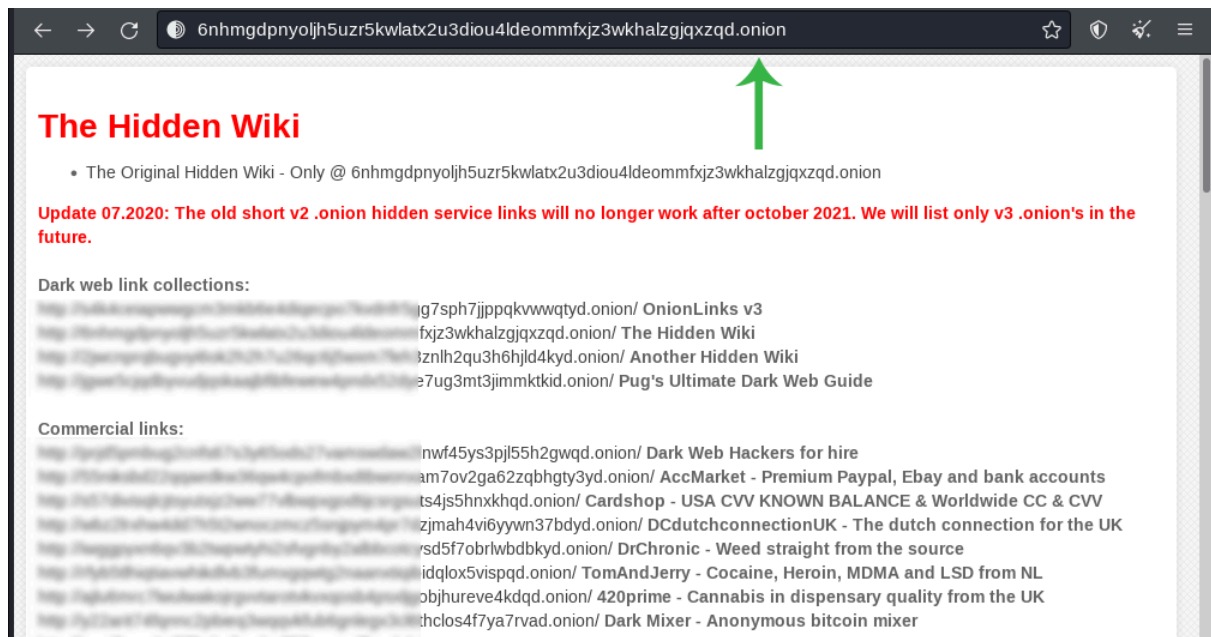
Jika Anda sudah selesai menghubungkan Tor Browser ke jaringan Tor, Anda dapat langsung mengunjungi:

<https://thehiddenwiki.org/cgi-sys/suspendedpage.cgi>
untuk menemukan daftar tautan ke berbagai situs di dark web.



Gambar di atas menampilkan halaman **Hidden Wiki** yang memuat daftar tautan situs **.onion** terbaru untuk diakses melalui jaringan Tor. Pada bagian **New .onion links 2021**, terlihat berbagai indeks situs yang mengarah ke berbagai layanan di dark web, termasuk salah satunya **The Hidden Wiki** (ditandai dengan panah hijau).

Sekarang klik salah satu tautan yang terindeks, yaitu yang berakhiran **.onion**. Setelah di klik, tautan tersebut akan mengarahkan Anda langsung ke halaman dark web terkait. Pada contoh ini, kita memilih tautan **The Hidden Wiki** untuk melanjutkan eksplorasi.



Tangkapan layar ini menunjukkan tampilan **Tor Browser** saat mengakses salah satu situs di jaringan *dark web*.

Terlihat pada bilah alamat (search bar) bahwa pengguna sedang berada di **The Hidden Wiki** melalui alamat domain versi 3 (.onion)

6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion.

The Hidden Wiki dikenal sebagai salah satu direktori populer yang memuat berbagai tautan ke situs-situs lain di *dark web*, termasuk koleksi *dark web links* dan tautan komersial. Pada halaman ini juga terdapat pemberitahuan penting bahwa mulai Oktober 2021, tautan *hidden service* versi 2 (.onion v2) tidak lagi berfungsi, dan hanya akan menampilkan tautan versi 3 (.onion v3) di masa mendatang.

Seperti terlihat pada bilah alamat, kita telah diarahkan ke halaman **The Hidden Wiki** di *dark web*.

Bab: Simulasi & Latihan Etis Mengakses Darkweb di Lingkungan Aman

Darkweb sering diasosiasikan dengan aktivitas ilegal, namun teknologi dan konsep yang digunakan di dalamnya juga memiliki sisi edukatif yang penting. Melalui simulasi di lingkungan yang aman dan terisolasi, seperti jaringan internal atau lab virtual, kita dapat mempelajari prinsip **keamanan**, **anonimitas**, dan **enkripsi** tanpa melanggar hukum. Latihan ini membantu profesional keamanan siber memahami potensi ancaman dan teknik yang digunakan, sehingga dapat memperkuat sistem pertahanan.

Tujuan Pembelajaran

Latihan ini dirancang untuk:

1. **Memahami arsitektur dan lapisan jaringan** (Surface Web, Deep Web, Dark Web).
2. **Menggunakan Kali Linux** untuk simulasi koneksi ke jaringan anonimitas seperti Tor.
3. **Menguji teknik keamanan dan enkripsi** secara praktis.
4. **Melatih etika profesional** dalam eksplorasi dunia maya.
5. **Mengidentifikasi risiko dan mitigasinya** di dunia nyata.

Lingkungan Aman untuk Simulasi

Jaringan Internal (Isolated Network)

- Menggunakan router atau switch yang tidak terhubung ke internet publik.
- Menjalankan **DNS lokal** dan server simulasi untuk meniru layanan yang seolah-olah berada di “darkweb”.
- Cocok untuk simulasi lalu lintas Tor dan hidden services secara terkendali.

Lab Virtual

- Memanfaatkan platform seperti **VirtualBox**, **VMware**, atau **Proxmox** untuk membuat beberapa mesin virtual:
 - **VM Kali Linux** untuk simulasi serangan/pengujian.
 - **VM Server Tor** untuk menyediakan layanan onion simulasi.
 - **VM Client** untuk mengakses layanan tersebut.
- Semua VM berada pada **Virtual Network** yang tidak memiliki koneksi keluar.

Langkah Simulasi Etis

Menyiapkan Kali Linux

1. Instal Kali Linux di VM.
2. Pastikan update paket dilakukan sebelum memutuskan koneksi dari internet publik.
3. Aktifkan mode jaringan **Host-Only Adapter**.

Menjalankan Tor di Lingkungan Aman

1. Install Tor (`sudo apt install tor`).
2. Konfigurasi file `torrc` untuk membuat layanan onion lokal.
3. Menyediakan **web server dummy** (misalnya menggunakan Apache atau Nginx) yang berisi halaman edukasi.

Mengakses Layanan Onion

1. Gunakan **Tor Browser** di VM klien untuk mengakses alamat `.onion` yang telah dibuat.
2. Pantau lalu lintas dengan **Wireshark** atau `tcpdump` untuk menganalisis proses enkripsi.

Simulasi Ancaman

- Buat “phishing page” atau “malware sample” fiktif (tidak berbahaya) untuk mengedukasi bagaimana serangan dapat muncul di darkweb.
- Analisis log dan pola trafik untuk mendeteksi anomali.

Prinsip Keamanan, Anonimitas, dan Enkripsi

Keamanan

- Penggunaan **sandboxing** untuk mencegah exploit keluar dari lingkungan simulasi.
- Mengisolasi VM secara ketat dari jaringan produksi.

Anonimitas

- Mempelajari prinsip routing berlapis Tor.
- Menguji perbedaan koneksi langsung vs. koneksi melalui node perantara.

Enkripsi

- Melihat bagaimana TLS/SSL bekerja di layanan onion.
- Memahami peran end-to-end encryption di jalur komunikasi.

Etika & Kepatuhan Hukum

- Tidak pernah mengakses konten ilegal.
- Menggunakan hanya **sumber daya internal** yang aman.
- Memastikan semua peserta memahami batasan hukum di negara masing-masing.
- Dokumentasi setiap langkah untuk transparansi dan pembelajaran.

Penutup

Simulasi ini memberikan kesempatan untuk belajar dari teknologi yang digunakan di darkweb tanpa melanggar hukum. Dengan menggunakan Kali Linux di lingkungan terisolasi, peserta dapat memperdalam pemahaman tentang keamanan, anonimitas, dan enkripsi, sekaligus mengasah keterampilan investigasi digital secara etis.

BAB: Akses Situs Dark Web

Akses Situs Dark Web

- Di Tor Browser, kunjungi situs .onion (alamat dark web berakhir dengan .onion).
- Mulai dengan direktori aman seperti The Hidden Wiki: Ketik http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page atau cari versi terbaru.
- Hindari link acak; verifikasi dari sumber terpercaya.

Mencari Informasi di Dark Web

- Gunakan mesin pencari khusus dark web (search engine .onion) untuk menemukan informasi. Beberapa yang direkomendasikan di 2025:
 - **Ahmia:**
<http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/> – Fokus pada pencarian aman dan bebas spam.
 - **Torch:**
<http://xmh57jrknzkxhv6y3ls7u4xel6qgzoi4unmnnbsdzsqwez463vq2ghqk5.onion/> – Salah satu yang tertua, indeks jutaan halaman.
 - **DuckDuckGo Onion:**
<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/> – Versi anonim DuckDuckGo, bagus untuk pencarian dasar.
 - **Haystak:**
<http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22geiyeiaehe2zid.onion/> – Indeks besar, mendukung pencarian mendalam.
 - **Not Evil:** <http://hss3uro2hsxfogfq.onion/> – Sederhana dan cepat, mirip Google tapi untuk dark web.
- Cara mencari: Masukkan kata kunci di search engine tersebut, seperti "cybersecurity forums" atau topik spesifik. Hasil akan berupa link .onion.
- Gunakan tabel untuk perbandingan singkat:

Search Engine	Kelebihan	Kekurangan
Ahmia	Aman, filter spam	Lebih lambat
Torch	Indeks besar	Banyak iklan
DuckDuckGo	Mudah digunakan	Tidak khusus dark web
Haystak	Pencarian mendalam	Berbayar untuk fitur premium
Not Evil	Cepat dan sederhana	Kurang fitur

Tips Keamanan Tambahan

- **Gunakan VPN + Tor:** Jalankan VPN dulu, lalu Tor, untuk "double hop" anonimitas.
- Nonaktifkan JavaScript jika tidak perlu (di pengaturan Tor > Security Level > Safest).
- Jangan login akun pribadi atau transfer data sensitif.
- Update Tor secara berkala via launcher.
- Jika ragu, tutup browser dan mulai ulang sesi baru.
- Hindari situs ilegal; fokus pada forum edukasi seperti Reddit onion atau wiki anonim.

Jika mengalami error, periksa log Tor atau reinstall paket. Untuk panduan video, cari tutorial terbaru di YouTube. Selamat menjelajah secara aman!

Memahami Alamat .onion dan Mencari Informasi

Situs di *dark web* tidak menggunakan domain seperti **.com** atau **.org**. Sebaliknya, mereka menggunakan *top-level domain* khusus yang disebut **.onion**. Alamat ini adalah serangkaian karakter acak, contohnya <http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyc1en53wid.onion/> (ini adalah alamat untuk DuckDuckGo versi *onion*).

Anda tidak bisa begitu saja mencari situs **.onion** di Google. Anda memerlukan mesin pencari (*search engine*) khusus *dark web*.

Mesin Pencari Populer di Dark Web

- **Ahmia:** Ini adalah salah satu mesin pencari **.onion** yang paling populer dan andal. Ahmia berfokus pada pengindeksan situs yang tidak mengandung konten ilegal atau berbahaya.
 - **Alamat Clearnet (bisa diakses dari browser biasa):** ahmia.fi
 - **Alamat Onion (akses dari Tor Browser):**
<http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibso4t4csyd.onion/>
- **DuckDuckGo (Versi Onion):** Mesin pencari yang berfokus pada privasi ini juga memiliki versi **.onion**. Meskipun tidak secara khusus mengindeks situs **.onion** sebanyak Ahmia, ia tidak akan melacak pencarian Anda.
 - **Alamat Onion:**
<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twag5wzczad.onion/>
- **The Hidden Wiki:** Ini bukan mesin pencari, melainkan direktori tautan yang dikelola oleh komunitas. Ini adalah titik awal yang baik untuk menemukan berbagai jenis situs. Namun, **berhati-hatilah**, karena The Hidden Wiki sering kali menautkan ke situs-situs yang berisi konten ilegal dan berbahaya. Selalu ada beberapa versi "The Hidden Wiki," beberapa di antaranya adalah tiruan berbahaya.

Cara Praktis Mencari Informasi

1. Buka Tor Browser.

2. Masukkan alamat mesin pencari seperti Ahmia (<http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/>) ke bilah alamat.
3. Setelah halaman Ahmia terbuka, gunakan bilah pencariannya untuk memasukkan kata kunci yang Anda cari, sama seperti menggunakan Google.
4. Hasil pencarian akan menampilkan daftar situs [.onion](#) yang relevan. Klik tautan untuk mengunjunginya.

BAB: [DarkRadar.io](https://darkradar.io)

DarkRadar.io adalah platform Cyber Threat Intelligence (CTI) yang dikembangkan oleh CyberArmyID, sebuah perusahaan keamanan siber asal Indonesia di bawah naungan PT Global Inovasi Siber Indonesia. Platform ini dirancang untuk memantau, mendeteksi, dan memberikan peringatan dini terhadap ancaman siber, khususnya yang berasal dari dark web dan aktivitas siber lainnya. Berikut adalah penjelasan tentang DarkRadar.io berdasarkan informasi yang tersedia:

Fitur Utama DarkRadar.io

1. **Pemantauan Dark Web (Dark Web Monitoring):**
 - DarkRadar.io memindai dark web untuk mendeteksi kebocoran data sensitif, seperti kredensial, dokumen rahasia, atau informasi pelanggan yang diperjualbelikan. Platform ini memberikan laporan terperinci untuk membantu organisasi menilai dampak kebocoran dan mengambil tindakan pencegahan.
 - Fitur ini juga memungkinkan deteksi dini terhadap data yang bocor, seperti email atau kata sandi, sehingga pengguna dapat mengganti kredensial sebelum disalahgunakan.
2. **Threat Hunting dan Analisis Ancaman:**
 - Menggunakan teknologi big data dan kecerdasan buatan (AI), DarkRadar.io memberikan wawasan ancaman secara real-time dengan analisis kontekstual mendalam. Ini termasuk mendeteksi serangan zero-day, Advanced Persistent Threats (APT), serta pola taktik, teknik, dan prosedur (TTPs) yang digunakan oleh pelaku kejahatan siber.
 - Platform ini memantau diskusi di forum peretas dan pasar dark web untuk mengidentifikasi ancaman sebelum serangan terjadi, seperti penjualan celah keamanan atau rencana serangan.
3. **Pemantauan Pelanggaran Data Perusahaan:**
 - DarkRadar.io menawarkan fitur pemantauan pelanggaran data perusahaan, yang memungkinkan organisasi untuk melacak dokumen rahasia atau informasi sensitif yang bocor di dark web. Ini membantu perusahaan mengurangi risiko eksploitasi data.
4. **Pemantauan Aktivitas Ransomware:**
 - Platform ini memantau komunikasi antara penyerang dan korban ransomware, mendeteksi permintaan pembayaran, kunci enkripsi, dan ancaman ransomware yang sedang berkembang, sehingga organisasi dapat mengambil tindakan proaktif.
5. **Perlindungan Merek dan Deteksi Phishing:**
 - DarkRadar.io dilengkapi dengan kemampuan deteksi phishing tingkat lanjut, pemindaian internet menyeluruh, dan deteksi kredensial yang dikompromikan. Ini membantu organisasi melindungi aset digital mereka dari ancaman seperti domain palsu atau email phishing.
6. **External Attack Surface Management (EASM):**

- Modul EASM secara otomatis memetakan lanskap digital organisasi tanpa perlu inventaris manual, membantu mengidentifikasi dan mengelola potensi risiko siber di permukaan serangan eksternal.
7. **Pemeriksaan Kebocoran Data Pribadi:**
- Pengguna individu dapat memeriksa apakah alamat email mereka telah bocor dalam insiden pelanggaran data. DarkRadar.io menjamin bahwa informasi email yang dimasukkan tidak disimpan, menjaga privasi pengguna.

Keunggulan DarkRadar.io

- **Real-Time dan Proaktif:** Memberikan peringatan dini dan wawasan ancaman secara cepat, memungkinkan organisasi untuk bertindak sebelum ancaman siber menjadi serangan nyata.
- **Skala Besar:** Menganalisis lebih dari 300 miliar data dengan mendeteksi lebih dari 85 miliar kebocoran data, menunjukkan kemampuan pemrosesan data yang masif.
- **Sertifikasi Keamanan:** DarkRadar.io dioperasikan oleh CyberArmyID yang telah tersertifikasi ISO/IEC 27001:2022, menjamin standar keamanan informasi yang tinggi.
- **Integrasi dengan Ekosistem CyberArmyID:** DarkRadar.io merupakan bagian dari solusi keamanan siber yang lebih luas dari CyberArmyID, termasuk platform seperti CyberAcademyID, Helium.sh, dan CyberPhishing.id, yang mendukung pendidikan siber, pengujian keamanan otomatis, dan simulasi phishing.

Konteks CyberArmyID

CyberArmyID adalah perusahaan inovasi keamanan siber yang berfokus pada perlindungan sistem digital, jaringan, dan data dari ancaman siber. Mereka menawarkan berbagai layanan seperti Bug Bounty Program, pelatihan keamanan siber, dan pengujian keamanan otomatis. DarkRadar.io adalah salah satu produk unggulan mereka yang dikhususkan untuk intelijen ancaman siber. Perusahaan ini juga telah bekerja sama dengan berbagai klien, termasuk pemerintah dan sektor swasta, seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Luar Negeri, dan perusahaan seperti BPJS dan Kitabisa.

Manfaat untuk Pengguna

- **Organisasi:** Membantu perusahaan dan instansi pemerintah mendeteksi ancaman siber lebih awal, melindungi data sensitif, dan memperkuat pertahanan digital mereka.
- **Individu:** Memberikan alat untuk memeriksa kebocoran data pribadi dan saran tindakan pencegahan, seperti mengaktifkan autentikasi dua faktor (2FA) atau menggunakan pengelola kata sandi.
- **Keamanan Proaktif:** Dengan memanfaatkan intelijen ancaman, pengguna dapat mengenali pola serangan seperti phishing atau serangan zero-day sebelum menyebabkan kerusakan.

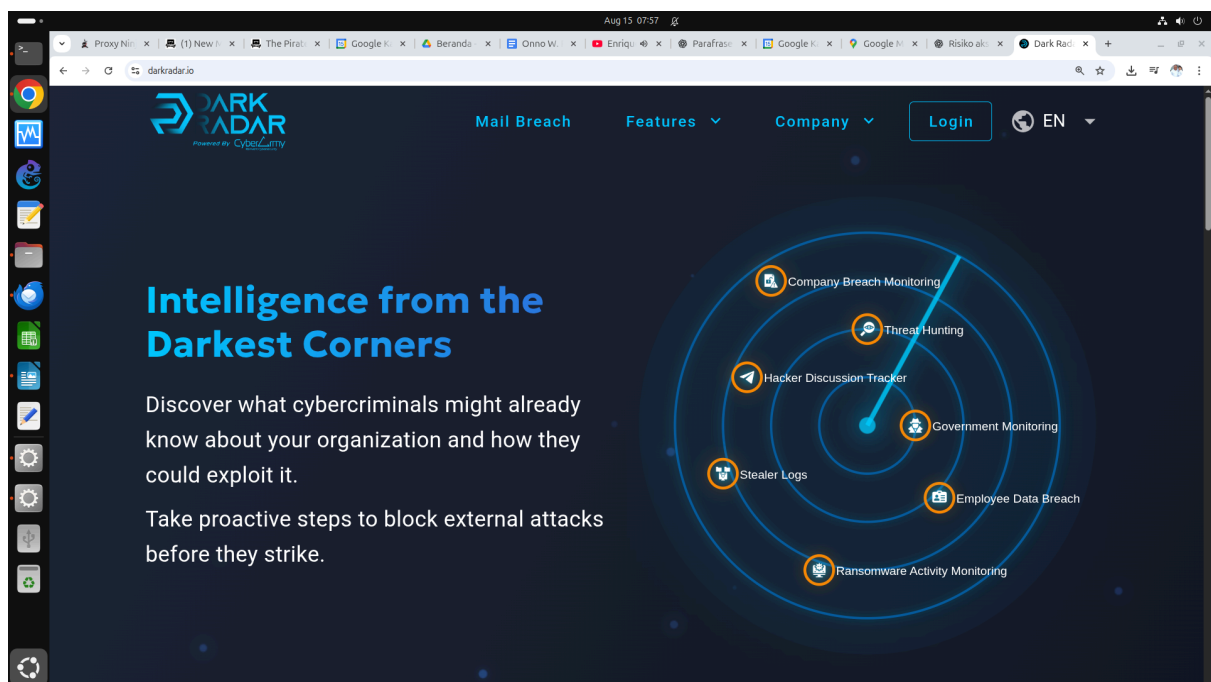
Cara Menggunakan DarkRadar.io

- Pengguna dapat mengakses fitur seperti pemeriksaan kebocoran email melalui situs web resmi (www.darkradar.io).
- Untuk organisasi, DarkRadar.io menawarkan demo dan integrasi API untuk solusi keamanan yang lebih komprehensif.
- Platform ini juga menyediakan laporan ancaman dan rekomendasi tindakan untuk membantu pengguna mengatasi risiko siber.

Kesimpulan

DarkRadar.io adalah solusi Cyber Threat Intelligence yang canggih dan proaktif, dibuat oleh CyberArmyID untuk melindungi organisasi dan individu dari ancaman siber yang kompleks. Dengan fitur seperti pemantauan dark web, deteksi phishing, dan analisis ancaman berbasis AI, platform ini membantu pengguna tetap selangkah lebih maju dari pelaku kejahatan siber. Untuk informasi lebih lanjut atau mencoba demo, kunjungi www.darkradar.io.

Praktek Menggunakan DarkRadar



Pada layar utama **DarkRadar.io**, pengguna langsung disambut dengan nuansa gelap bernuansa futuristik, menonjolkan tema “dark web intelligence”. Di sisi kiri layar, terdapat logo **DarkRadar** dengan tagline *Powered by CyberLymy*, menegaskan identitas dan sumber teknologinya.

Bagian utama halaman menampilkan judul besar **"Intelligence from the Darkest Corners"** dengan teks berwarna biru cerah, memberikan kontras yang kuat terhadap latar belakang gelap. Tepat di bawahnya, terdapat deskripsi singkat yang menjelaskan tujuan layanan ini: membantu organisasi mengetahui informasi yang mungkin sudah dikantongi oleh para

pelaku kejahatan siber dan bagaimana cara mereka memanfaatkannya, serta mendorong langkah proaktif untuk mencegah serangan sebelum terjadi.

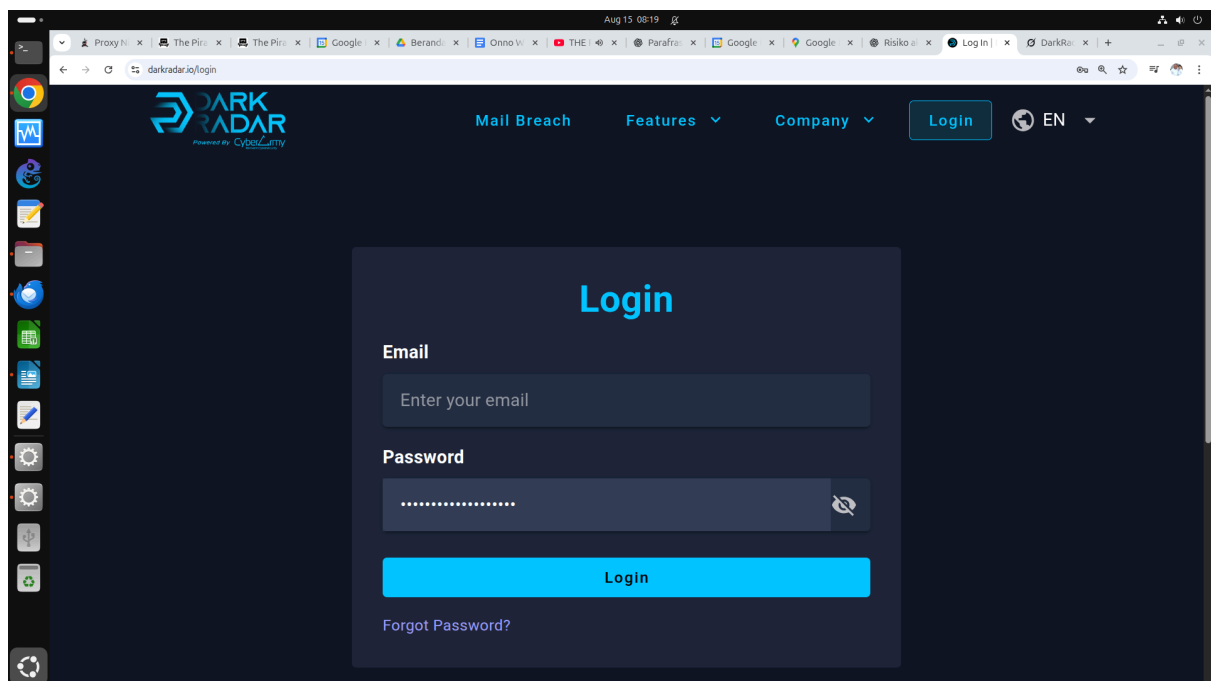
Di sisi kanan, terdapat ilustrasi radar digital dengan lingkaran konsentris dan titik-titik ikon yang mewakili fitur-fitur utama:

- **Company Breach Monitoring**
- **Threat Hunting**
- **Hacker Discussion Tracker**
- **Government Monitoring**
- **Stealer Logs**
- **Employee Data Breach**
- **Ransomware Activity Monitoring**

Ikon-ikon ini dilengkapi simbol visual yang relevan, dilingkari warna orange untuk menonjolkan fokus monitoring. Animasi radar ini memberikan kesan “mendeteksi ancaman” secara real-time.

Navigasi utama terletak di bagian atas, dengan menu seperti **Mail Breach**, **Features**, **Company**, serta tombol **Login** berbingkai biru. Disampingnya, terdapat pilihan bahasa (default: EN) untuk memudahkan pengguna internasional.

Secara keseluruhan, desain ini mengkomunikasikan kesan profesional, misterius, dan penuh kewaspadaan—sesuai dengan misi DarkRadar untuk mengungkap intelijen dari sudut tergelap dunia maya.

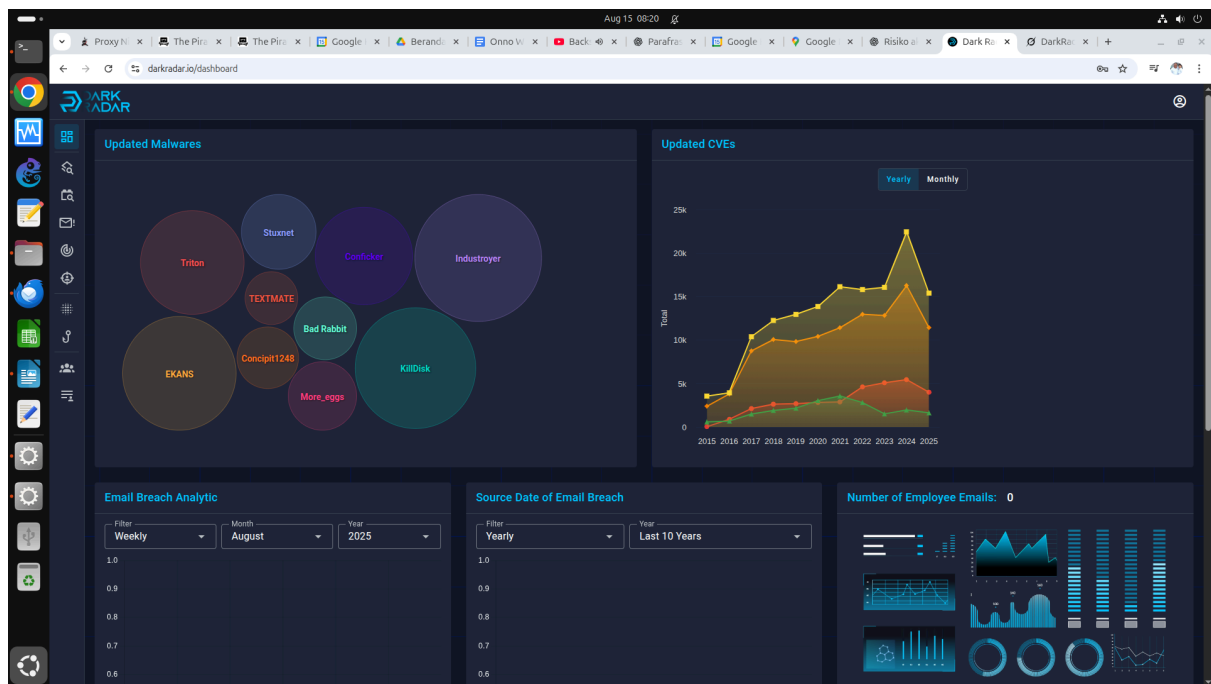


Halaman login DarkRadar.io menampilkan antarmuka sederhana namun profesional, dengan dominasi warna gelap dan aksen biru yang menonjolkan elemen penting. Di bagian tengah terdapat form login yang terdiri dari dua kolom utama: **Email** dan **Password**. Pengguna diminta untuk memasukkan alamat email yang terdaftar serta kata sandi rahasia mereka.

Tombol **Login** berwarna biru terang berada di bawah form, menjadi fokus utama untuk memulai proses autentikasi.

Sebagai langkah keamanan tambahan, DarkRadar.io menerapkan kebijakan **Two-Factor Authentication (2FA)** wajib. Setelah berhasil memasukkan email dan kata sandi, pengguna tidak langsung masuk ke akun. Sistem akan meminta verifikasi kode keamanan sekali pakai (OTP) yang dihasilkan oleh aplikasi **Authenticator** di perangkat Android pengguna. Aplikasi ini, seperti Google Authenticator atau Authy, memberikan kode unik yang terus diperbarui setiap 30 detik, sehingga meminimalkan risiko pembobolan meskipun kata sandi utama diketahui pihak tidak berwenang.

Dengan kombinasi kata sandi dan kode OTP dari Authenticator Android, proses login di DarkRadar.io memastikan keamanan ganda yang melindungi data sensitif dari ancaman siber, khususnya mengingat platform ini berhubungan dengan informasi keamanan dan pemantauan dark web.



Tangkapan layar ini menampilkan antarmuka **DarkRadar**, sebuah platform intelijen keamanan siber yang memantau ancaman seperti malware terbaru, kerentanan (CVE), dan insiden kebocoran data email. Tampilan dashboard menggunakan tema gelap dengan visualisasi data interaktif.

Updated Malwares

Bagian kiri atas menunjukkan **visualisasi bubble chart** yang menampilkan berbagai malware terbaru.

- Ukuran gelembung mencerminkan tingkat signifikansi atau jumlah laporan aktivitas malware tersebut.

- Contoh malware yang terdeteksi: **Triton**, **EKANS**, **KillDisk**, **Industroyer**, **Stuxnet**, **Bad Rabbit**, **Conficker**, dan lainnya.
- Warna berbeda kemungkinan mewakili kategori atau tingkat ancaman.

Updated CVEs

Di kanan atas terdapat **grafik tren kerentanan (CVE)** dari tahun 2015 hingga 2025.

- Sumbu X menunjukkan tahun, sumbu Y menunjukkan jumlah total CVE yang diperbarui.
- Terlihat tren kenaikan signifikan sejak 2017, dengan puncak tertinggi pada sekitar 2024, lalu sedikit menurun pada 2025.
- Grafik ini memiliki opsi filter **Yearly** dan **Monthly** untuk melihat data secara tahunan atau bulanan.

Email Breach Analytic

Bagian kiri bawah menampilkan **grafik analitik kebocoran email** yang dapat difilter berdasarkan:

- Periode (Weekly)
- Bulan (Agustus)
- Tahun (2025)

Pada screenshot ini, grafik menunjukkan nilai mendekati nol, mengindikasikan tidak ada atau sangat sedikit insiden untuk periode tersebut.

Source Date of Email Breach

Tengah bawah menampilkan grafik sumber tanggal kebocoran email, dengan filter:

- Periode (Yearly)
- Rentang waktu (Last 10 Years)

Data pada gambar juga terlihat kosong atau mendekati nol.

Number of Employee Emails

Pojok kanan bawah memperlihatkan jumlah email pegawai yang terdeteksi dalam insiden kebocoran, yang pada screenshot ini bernilai **0**.

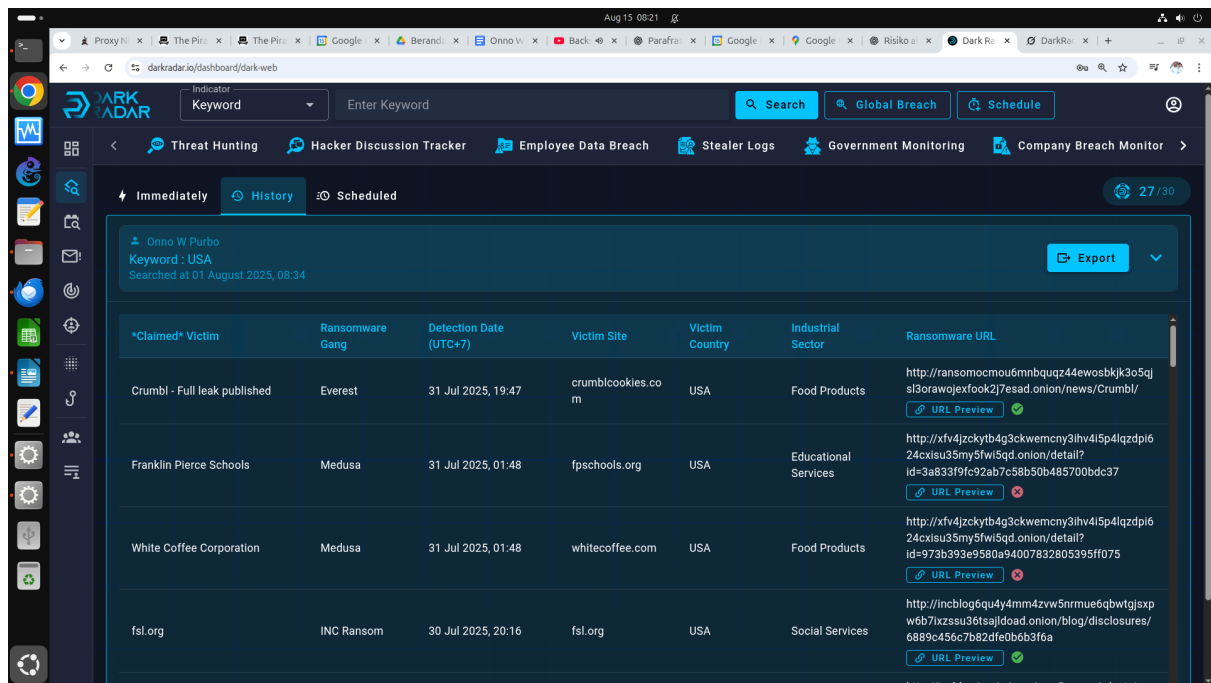
Bagian ini juga menampilkan beberapa **visualisasi mini** (sparkline, bar chart, dan pie chart) untuk memberikan insight tambahan jika data tersedia.

Kesimpulan

Dashboard ini menunjukkan bahwa:

- Ada pemantauan aktif terhadap malware dan kerentanan terbaru.
- Tren CVE terus meningkat dalam dekade terakhir, dengan lonjakan besar di 2024.

- Untuk periode Agustus 2025, tidak ada kebocoran email pegawai yang terdeteksi.
- Data yang ditampilkan memungkinkan tim keamanan untuk cepat mengidentifikasi ancaman, memantau tren, dan mengambil tindakan mitigasi.



Gambar ini menampilkan antarmuka aplikasi **DarkRadar**, sebuah platform pemantauan dark web yang digunakan untuk melacak insiden kebocoran data, aktivitas ransomware, serta ancaman siber lainnya. Pada tangkapan layar ini, tab yang aktif adalah **History**, yang menampilkan hasil pencarian dengan kata kunci "**USA**" yang dilakukan pada **1 Agustus 2025 pukul 08:34 (UTC+7)** oleh pengguna bernama *Onno W Purbo*.

Tabel utama pada layar berisi informasi terperinci terkait insiden ransomware yang menargetkan berbagai organisasi di Amerika Serikat. Kolom-kolom yang tersedia antara lain:

1. **Claimed Victim**
Menunjukkan nama atau domain organisasi yang menjadi korban dan status kebocoran (misalnya *Full leak published*).
2. **Ransomware Gang**
Mengidentifikasi kelompok peretas atau geng ransomware yang mengklaim bertanggung jawab atas serangan (contohnya: *Everest*, *Medusa*, *INC Ransom*).
3. **Detection Date (UTC+7)**
Waktu dan tanggal deteksi insiden berdasarkan zona waktu UTC+7.
4. **Victim Site**
Domain situs web organisasi korban.
5. **Victim Country**
Negara target, yang dalam semua entri di tabel ini adalah **USA**.

6. **Industrial Sector**

Sektor industri yang terdampak (misalnya *Food Products*, *Educational Services*, *Social Services*).

7. **Ransomware URL**

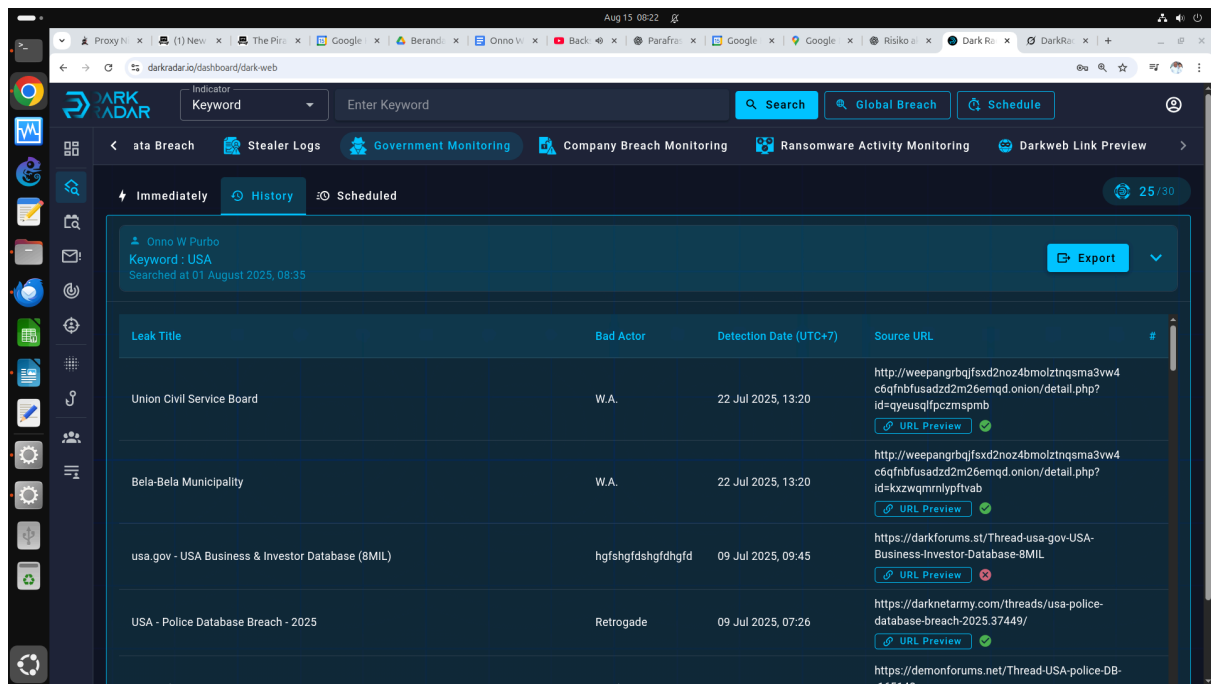
Tautan menuju halaman *dark web* yang memuat informasi kebocoran. Sebagian tautan disertai opsi **URL Preview** yang memungkinkan peninjauan isi sebelum membuka alamat .onion tersebut.

Beberapa contoh insiden pada tabel ini:

- **Crumbl** (*Food Products*)
Diserang oleh geng ransomware *Everest*, dengan status *full leak published* pada 31 Juli 2025, 19:47. Situs korban adalah crumblcookies.com.
- **Franklin Pierce Schools** (*Educational Services*)
Diserang oleh *Medusa*, terdeteksi pada 31 Juli 2025, 01:48. Domain korban adalah fpschools.org.
- **White Coffee Corporation** (*Food Products*)
Juga diserang oleh *Medusa*, dengan waktu deteksi yang sama seperti kasus Franklin Pierce Schools.
- **FSL.org** (*Social Services*)
Menjadi korban geng *INC Ransom*, terdeteksi pada 30 Juli 2025, 20:16.

Tampilan seperti ini berguna untuk:

- **Pemantauan ancaman** — membantu tim keamanan siber melacak klaim kebocoran yang muncul di dark web.
- **Analisis insiden** — mengidentifikasi pola target serangan, sektor industri yang rentan, serta kelompok ransomware yang aktif.
- **Respon cepat** — menyediakan URL sumber di dark web agar dapat dilakukan validasi dan investigasi lebih lanjut.



Tangkapan layar ini memperlihatkan tampilan dashboard **DarkRadar** pada tab **History** di bagian **Data Breach** dengan kata kunci pencarian "**USA**". Pencarian dilakukan oleh pengguna bernama **Onno W Purbo** pada **1 Agustus 2025** pukul **08:35**.

Bagian utama tabel berisi daftar temuan kebocoran data (*leak*) yang terdeteksi di dark web, lengkap dengan kolom **Leak Title**, **Bad Actor**, **Detection Date (UTC+7)**, dan **Source URL**. Beberapa contoh entri yang terlihat antara lain:

1. **Union Civil Service Board**
 - Bad Actor: W.A.
 - Deteksi: 22 Juli 2025, 13:20
 - Sumber: Tautan [.onion](#) di dark web.
2. **Bela-Bela Municipality**
 - Bad Actor: W.A.
 - Deteksi: 22 Juli 2025, 13:20
 - Sumber: Tautan [.onion](#) di dark web.
3. **usa.gov – USA Business & Investor Database (8MIL)**
 - Bad Actor: hgfshgfdshgfdhgfd
 - Deteksi: 09 Juli 2025, 09:45
 - Sumber: Forum *darkforums.st*.
4. **USA – Police Database Breach – 2025**
 - Bad Actor: Retrogade
 - Deteksi: 09 Juli 2025, 07:26
 - Sumber: *darknetarmy.com*.

5. **USA – police DB**

- Bad Actor: BeadH09
- Deteksi: 09 Juli 2025, 10:09
- Sumber: *demonforums.net*.

Setiap entri memiliki opsi **URL Preview** untuk meninjau tautan sumber, beberapa di antaranya menampilkan ikon tanda centang hijau (tautan aktif) atau tanda silang merah (tautan tidak aktif).

Di sisi kanan layar, terlihat tombol **Export** untuk mengunduh hasil pencarian, serta indikator kuota penggunaan (25/30). Menu navigasi di bagian atas menampilkan kategori pemantauan seperti **Government Monitoring**, **Company Breach Monitoring**, **Ransomware Activity Monitoring**, dan **Darkweb Link Preview**.

BAB: Praktik Terbaik untuk Keamanan dan Anonimitas di Dark Web

1. **Hindari Menggunakan Data Pribadi**

Jangan pernah membagikan nama asli, alamat email, kata sandi, atau informasi identitas pribadi lainnya saat menjelajah di dark web.

- **Contoh di komputer:** Saat mendaftar akun, gunakan username acak seperti **Bintang_92** dan email sementara dari layanan seperti *ProtonMail* atau *Guerrilla Mail*.
- **Contoh di Android:** Gunakan aplikasi email anonim seperti *Tutanota* yang bisa diunduh di Play Store untuk membuat alamat baru tanpa data asli.

2. **Biarkan Ukuran Jendela Browser Default**

Beberapa situs dapat melacak ukuran jendela browser. Dengan membiarkannya tetap pada ukuran bawaan Tor Browser, Anda akan “tenggelam” di antara pola pengguna lain, sehingga anonimitas lebih terjaga.

- **Contoh di komputer:** Jangan memaksimalkan atau mengecilkan jendela Tor Browser; biarkan apa adanya saat dibuka pertama kali.
- **Contoh di Android:** Gunakan mode potret (vertical) default, jangan ubah ke layar penuh jika tidak perlu.

3. **Jangan Mengaktifkan Plugin**

Tor Browser memblokir plugin seperti Flash, RealPlayer, atau QuickTime karena bisa dimanfaatkan untuk mengetahui alamat IP Anda.

- **Contoh di komputer:** Jangan instal ekstensi tambahan yang tidak resmi di Tor Browser.

- **Contoh di Android:** Jika diminta mengaktifkan pemutar media atau plugin tambahan, pilih “Tolak” atau “Batal”.

4. Selalu Gunakan HTTPS

Jika sebuah situs **.onion** menyediakan versi *HTTPS*, gunakan alamat tersebut untuk memastikan koneksi terenkripsi.

- **Contoh di komputer:** Periksa ikon gembok di bilah alamat Tor Browser sebelum memasukkan informasi apapun.
- **Contoh di Android:** Aktifkan pengaturan “HTTPS Only Mode” di Tor Browser Android.

5. Hati-Hati Saat Mengunduh

File dari sumber yang tidak jelas bisa mengandung malware atau program untuk melacak identitas Anda.

- **Contoh di komputer:** Jangan mengunduh file **.exe** atau **.doc** dari forum yang tidak dikenal. Jika harus mengunduh, gunakan mesin virtual (VM) untuk membukanya.
- **Contoh di Android:** Hindari mengunduh file APK langsung dari tautan yang tidak diverifikasi.

6. Gunakan VPN untuk Lapisan Keamanan Tambahan (Opsional)

Menghubungkan VPN sebelum membuka Tor (VPN over Tor) dapat menyembunyikan fakta bahwa Anda menggunakan Tor dari ISP Anda.

- **Contoh di komputer:** Jalankan aplikasi VPN seperti Mullvad atau ProtonVPN, baru kemudian buka Tor Browser.
- **Contoh di Android:** Aktifkan VPN bawaan Android atau aplikasi VPN resmi sebelum membuka Tor Browser.

7. Tutup Aplikasi Lain Saat Menggunakan Tor

Aplikasi lain bisa saja membocorkan data tanpa Anda sadari. Tutup semua program sebelum menjalankan Tor untuk aktivitas sensitif.

- **Contoh di komputer:** Di Kali Linux, tutup semua jendela aplikasi lain seperti Telegram atau browser biasa.
- **Contoh di Android:** Tutup semua aplikasi latar belakang melalui menu *Recent Apps* sebelum menjalankan Tor Browser.

Referensi

1. **Geek Institute. (n.d.). How to Set Up a Dark Web Server on Kali Linux Using Tor and Nginx.** Blog Geek Institute. Diakses dari <https://blog.geekinstitute.org/2025/05/how-to-set-up-dark-web-server-on-kali.html>
 - Sumber ini memberikan panduan langkah demi langkah untuk mengatur server Dark Web menggunakan Tor dan Nginx pada Kali Linux, mencakup instalasi, konfigurasi, dan langkah pengamanan.
2. **GeeksforGeeks. How to Access the Dark Web Using the TOR Browser in Kali Linux.** GeeksforGeeks. Diakses dari <https://www.geeksforgeeks.org/how-to-access-dark-web-using-tor-browser-kali-linux>
 - Artikel ini menjelaskan cara mengakses Dark Web dengan aman menggunakan Tor Browser di Kali Linux, termasuk langkah-langkah instalasi dan rekomendasi penggunaan VPN.
3. **Giangianna14. (n.d.). Handson Kali Linux - Tutorial Bahasa Indonesia.** GitHub. Diakses dari <https://github.com/giangianna14/handson-kali-linux>
 - Repositori ini menyediakan panduan komprehensif dalam bahasa Indonesia untuk mempelajari penetration testing dan ethical hacking menggunakan Kali Linux, yang mencakup aspek-aspek keamanan jaringan relevan dengan Dark Web.
4. **Doel, M. (2016). Panduan Hacking Website dengan Kali Linux.** Elex Media Komputindo.
 - Buku ini membahas teknik-teknik hacking website dari tingkat dasar hingga menengah menggunakan Kali Linux, yang dapat menjadi dasar untuk memahami keamanan siber dan eksplorasi Dark Web.
5. **Damon Garn. (2025). Top 21 Kali Linux tools and how to use them.** Tech Target. Diakses dari <https://www.techtarget.com/searchsecurity/tip/Top-Kali-Linux-tools-and-how-to-use-them>
 - Sumber ini menjelaskan alat-alat utama dalam Kali Linux yang dapat digunakan untuk menjelajahi Dark Web, seperti Nmap, Wireshark, dan lainnya, dengan fokus pada penggunaan yang aman dan etis.

Catatan:

- Pastikan untuk menggunakan sumber-sumber ini hanya untuk tujuan pembelajaran dan ethical hacking. Aktivitas ilegal di Dark Web dapat memiliki konsekuensi hukum serius.
- Beberapa sumber, seperti tutorial GitHub, mungkin memerlukan pengetahuan dasar Linux dan jaringan untuk memahami konten secara maksimal.
- Jika Anda membutuhkan sumber tambahan atau panduan lebih spesifik, silakan beri tahu saya!

Tentang Penulis



Onno W. Purbo, saat ini bertugas sebagai rektor di Institut Teknologi Tangerang Selatan (ITTS). Onno memperoleh gelar Ph.D bidang Electrical Engineering dari University of Waterloo, Canada, adalah seorang copyleft, educator dan ICT evangelist. Dia sudah mempublikasikan 50++ buku, termasuk free ICT ebook untuk sekolah tahun 2008. Beberapa buku terakhirnya adalah "Internet-TCP/IP: Konsep Dan Implementasi", 2018; "Sistem Operasi, Konsep Dan Membuat Linux OpenWRT Dan ROM Android", 2019; "IPv6 Untuk Mendukung Operasi Jaringan Dan Domain Name System", 2019; "Kubernetes untuk Pemula", 2024 dan "Membuat Operator Seluler 5G Sendiri", 2024. Dia memimpin sambungan pertama Internet di Institut Teknologi Bandung, tahun 1993-2000, dan menggunakannya untuk membuat jaringan Internet pendidikan yang pertama di Indonesia. Dia membebaskan frekuensi WiFi, memperkenalkan RT/RW-net, antenna Wajanbolic dan jaringan selular OpenBTS dan private 5G sendiri. Dia memimpin jaringan telepon pertama di atas Internet, VoIP Merdeka, yang kemudian hari dikenal sebagai VoIP Rakyat berbasis SIP dan menggunakan kode area +62520 dan +62521. Dia saat ini aktif memperkenalkan e-Learning, dan menjalankan server e-Learning di <http://lms.onnocenter.or.id/moodle/> 66,000++ siswa / mahasiswa dan <https://opencourse.itts.ac.id> 36.000+ mahasiswa secara gratis. Email: onno@indo.net.id