Tools Reconnaissance Dan Scanning

Oleh:

Nama : Zumardi Irfan
NIM : 09040581721014
Prodi : TKJ4
Mata Kuliah : Keamanan Jaringan Komputer
Dosen Pengampu : Deris Stiawan, M.T., Ph.D.

FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

Whois

Apa itu whois?. Whois atau disuarakan “who is” digunakan untuk mendapatkan data informasi domain tertentu seperti nama pemilik domain, ip address, name server dan umur domain. Whois lookup yaitu sebuah aplikasi berbasis command line digunakan untuk melakukan query terhadap database whois.

Namun dalam perkembangannya, data whois suatu domain bisa dilihat di situs whois seperti domaintools atau whois.net. Sehingga user biasa seperti kita bisa mendapatkan informasi kepemilikan suatu domain dengan mudah. Walaupun demikian program whois berbasis command-line masih sering digunakan oleh Administrator jaringan.

Kegunaan whois

Selain mendapatkan informasi suatu domain, whois memiliki kegunaan sebagai berikut :

Mendukung keamanan dan kestabilan dari internet dengan menyediakan informasi kontak yang bisa dihubungi yang berhubungan dengan jaringan, ISP, dan pemilik domain.
Untuk mendapatkan informasi ketersediaan domain. Sehingga jika domain tersedia dalam artian belum diregistrasi oleh orang lain, maka Anda bisa melakukan registrasi atas nama domain tersebut.
Mempermudah penegakan hukum dalam investigasi pelanggaran hukum dalam suatu negara, seperti terorisme, pornografi, perdagangan organ, dan illegal content.
Memfasilitasi pencarian data untuk hak cipta dan merk dagang
Memberikan kontribusi pada kepercayaan pengunjung ketika mengunjungi suatu situs, seperti situs ecommerce (toko online), lembaga sosial, atau perusahaan yang menawarkan produk jasa.
Bagaimana cara mendapatkan informasi whois?

Untuk root domain umum seperti .com, .net atau .org bisa didapatkan dengan mudah dengan menggunakan salah satu situs whois, seperti domaintools dan whois.net. Masukkan nama domain yang ingin Anda lacak, contohnya mariocahyadi.com. Kemudian tekan tombol Lookup. Setelah itu Anda akan mendapatkan informasi whois dari domain yang bersangkutan.

Sedangkan root domain yang merupakan domain suatu negara seperti .id, .de maka pencarian domain dibawah root domain ini mesti dilakukan di pengelola domain yang bersangkutan. contohnya untuk mendapatkan informasi whois domain .ac.id atau .co.id maka Anda bisa mengunjungi situs Whois .id.

Privacy policy

Ada aturan yang memungkinkan data whois dari suatu domain tidak tersedia secara umum. Tujuannya adalah supaya informasi whois ini tidak digunakan oleh para spammer atau scammer.

Internet Archive
adalah sebuah perpustakaan digital nirlaba yang memiliki misi "akses universal untuk semua pengetahuan." Internet Archive menyediakan penyimpanan permanen dan akses publik bebas untuk koleksi bahan digital, termasuk situs web, musik, gambar bergerak, dan hampir tiga juta buku domain publik. Pada Oktober 2012, koleksinya mencapai 10 petabita. Selain fungsi pengarsipannya, Internet Archive juga adalah sebuah organisasi aktivis, advokasi untuk internet yang bebas dan terbuka.

Internet Archive memungkinkan masyarakat untuk mengunggah dan menngunduh materi digital ke kluster data, tetapi sebagian besar datanya dikumpulkan secara otomatis oleh web crawler, yang bekerja untuk melestarikan web publik sebanyak mungkin. Arsip web, Wayback Machine, berisi lebih dari 150+ miliar tangkapan web,Internet Archive juga mengawasi salah satu proyek digitalisasi buku terbesar di dunia.

Deteksi SO
Salah satu fitur Nmap yang paling dikenal adalah deteksi SO dengan menggunakan fingerprint stack TCP/IP. Nmap mengirimkan serangkaian paket TCP dan UDP ke host remote dan menguji setiap bit paket responnya. Setelah melakukan serangkaian test seperti sampling TCP ISN, dukungan dan urutan opsi TCP, sampling ID IP, dan pemeriksaan ukuran jendela awal, Nmap membandingkan hasilnya ke database nmap-os-db yang berisi lebih dari seribu fingerprint SO yang dikenal dan mencetak detil SO bila terjadi kesesuaian. Setiap fingerprint menyertakan deskripsi SO tekstual dalam format bebas, klasifikasi yang memberikan nama vendor (misalnya Sun), SO di bawahnya (misalnya Solaris), generasi OS (misalnya 10), dan jenis device (fungsi umum, router, switch, konsol game, dsb.).

Jika Nmap tidak dapat menduga SO mesin, dan kondisinya bagus (misalnya paling tidak ditemukan satu port terbuka dan tertutup), Nmap akan memberikan URL yang dapat anda gunakan untuk menyerahkan fingerprint jika anda tahu (dengan pasti) SO yang berjalan di mesin itu. Dengan melakukan hal ini anda berkontribusi ke database sistem operasi yang dikenali Nmap dan karenanya ia akan lebih akurat.

Deteksi SO mengaktifkan beberapa tes lain yang menggunakan informasi yang dikumpulkan selama proses. Salah satunya adalah TCP Sequence Predictability Classification. Ukuran ini menentukan seberapa sulit memalsukan koneksi TCP ke host remote. Ia bermanfaat dalam mengeksploitasi relasi trust berbasis IP-sumber (rlogin, filter firewall, dsb) atau untuk menyembunyikan sumber serangan. Spoofing jenis ini jarang dilakukan lagi, namun banyak mesin masih rentan terhadapnya. Angka kesulitan aktualnya berdasarkan pada sampling statistik dan mungkin berfluktuasi. Umumnya lebih baik menggunakan klasifikasi bahasa Inggris seperti “worthy challenge” or “trivial joke”. Hal ini hanya dilaporkan dalam output normal dalam mode verbose (-v). Ketika digunakan mode verbose bersama dengan -O, pembuatan urutan ID IP ID juga dilaporkan. Kebanyakan mesin berada dalam kelas “incremental”, yang berarti mereka menaikkan field ID dalam header IP untuk setiap paket yang mereka kirim. Hal ini

membuat mereka rentan atas beberapa serangan spoofing dan pengumpulan informasi tingkat tinggi.

Informasi ekstra lain yang disertakan dalam deteksi SO adalah menduga waktu uptime target. Tekniknya menggunakan opsi timestamp TCP (RFC 1323) untuk menduga waktu terakhir mesin direboot. Dugaan dapat tidak akurat akibat counter timestamp tidak diinisialisasi ke nol atau counter overflow dan kembali ke awal, sehingga ia hanya dicetak dalam mode verbose.

WhatWeb
adalah pemindai web generasi berikutnya.

WhatWeb mengenali teknologi web termasuk sistem manajemen konten (CMS), platform blogging, paket statistik / analitik, perpustakaan JavaScript, server web, dan perangkat yang disematkan.

WhatWeb memiliki lebih dari 1000 plugin, masing-masing untuk mengenali sesuatu yang berbeda. WhatWeb juga mengidentifikasi nomor versi, alamat email, ID akun, modul kerangka kerja web, kesalahan SQL, dan banyak lagi.

Nmap
Nmap (“Network Mapper”) merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

Output Nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Hal kunci di antara informasi itu adalah “tabel port menarik”. Tabel tersebut berisi daftar angka port dan protokol, nama layanan, dan status. Statusnya adalah terbuka (open), difilter (filtered), tertutup (closed), atau tidak difilter (unfiltered). Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port digolongkan sebagai tidak difilter ketika mereka menanggapi probe Nmap, namun Nmap tidak dapat menentukan apakah mereka terbuka atau tertutup. Nmap melaporkan kombinasi status open|filtered dan closed|filtered ketika ia tidak dapat menentukan status manakah yang menggambarkan sebuah port. Tabel port mungkin juga menyertakan detil versi software ketika diminta melakukan pemeriksaan versi.

Ketika sebuah pemeriksaan protokol IP diminta (-sO), Nmap memberikan informasi pada protokol IP yang didukung alih-alih port-port yang mendengarkan.

Selain tabel port yang menarik, Nmap dapat pula memberikan informasi lebih lanjut tentang target, termasuk nama reverse DNS, prakiraan sistem operasi, jenis device, dan alamat MAC.

Social Engineering
pengertian Social engineering adalah manipulasi psikologis seseorang dengan tujuan untuk mendapatkan informasi tertentu atau melakukan hal tertentu dengan cara menipunya secara halus dan tidak dia sadari. manipulasi psikologis dikakukan dengan berbagai media yang tujuan nya untuk mempengaruhi pikiran korban,misalnya menggunakan suara (berbicara untuk meyakinkan korban),gambar(memasang gambar yang erotis agar di klik),tulisan (menulis artikel yang persuasif dan meyakinkan misal menulis tutorial cara hack akun facebook,tapi palsu :D)

Dengan kata lain Social engineering adalah tehnik untuk mendapatkan informasi /hak akses dengan cara menipu korban nya dengan halus dan tanpa dia sadari. Semua kriminal 100% menggunakan tehnik ini untuk mendapatkan informasi dari korban nya. mulai dari tukang copet yang menyamar sebagai penumpang biasa, penipu yang menjanjikan hal luar biasa pada korban nya,sexpredator yang menggunakan facebook untuk berinteraksi dengan korban nya. dan lain sebagainya.

Kenapa social engineering tehnik?
Social engineering mentargetkan rantai terlemah dalam sistem keamanan komputer,yaitu user atau pengguna atau manusia itu sendiri. Bug atau celah keamanan ini bersifat universal,
tidak tergantung platform,sistem operasi,protocol,software ataupun hardware. vulnerability disetiap sistemDengan artian,semua sistem tercanggih di planet ini memiliki celah keamanan tersebut.

Tidak semua pekerjahan hacking (menjebol sistem) murni dilakaukan dari balik layar atau hanya fokus meng exploitasi mesin,karena semakin berkembang nya zaman keamanan komputer juga semakin sulit ditembus.teknik ini banyak dipake untuk penyebaran malware atau mendapatkan informasi yang diperlukan hacker,seperti identitas seseorang.

Untuk mendapatkan sebuah akses ke sebuah sistem (komputer,gedung,relasi,komunitas,rasa percaya kita) bisa dilakukan dengan melakukan pendekatan dengan manusia itu sendiri untuk mendapatkan kepercayaan agar pelaku social engineer bisa melakukan apa yang dia inginkan tanpa korban sadari. ketika sadar itu sudah sangat terlambat. jadi yang disebut sistem disini bukan hanya komputer tetapi bisa juga pikiran kita sendiri,keamanan sebuah gedung,sebuah kommunitas dll.

Social engineering tehnik tidak hanya dilakukan oleh kriminal, tetapi polisi/penegak hukum juga menggunakan tehnik ini untuk memata-matai target operasi dan mendapatkan informasi tentang target operasi.

Injeksi SQL (SQL Injection)
SQL Injection adalah teknik yang menyalahgunakan celah keamanan yang ada pada lapisan basis data sebuah aplikasi. Celah ini terjadi ketika input dari pengguna tidak disaring secara benar, contohnya adalah kolom username yang seharusnya hanya diisi dengan huruf atau angka tapi malah diisi dengan karakter lain (seperti: – = ') sehingga penyerang menggunakan celah tersebut dengan cara memasukan query dari SQL.

SQL Injection selalu menjadi teknik penyerangan terfavorit sebagian besar hacker dari tahun ke tahun, disamping karena semakin sulitnya hacker melakukan serangan melalui jaringan yang disebabkan oleh semakin canggihnya perangkat-perangkat pertahanan dari target (contoh: firewall, IDS, UTM, dll), SQL Injection juga sangat mudah dilakukan karena masih banyak web programmer yang masih kurang "aware" terhadapnya.

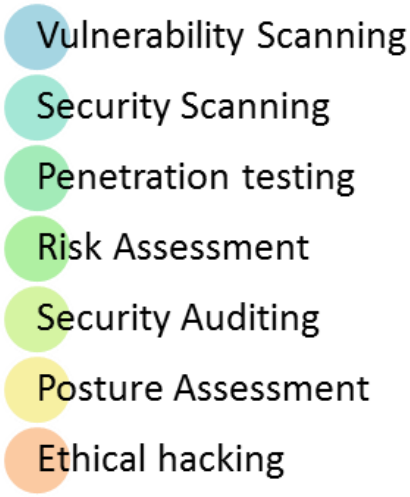
Apa itu Security Testing Methodology?

Pengujian Keamanan didefinisikan sebagai jenis Pengujian Perangkat Lunak yang memastikan sistem dan aplikasi perangkat lunak bebas dari segala kerentanan, ancaman, risiko yang dapat menyebabkan kerugian besar. Pengujian keamanan sistem apa pun adalah tentang menemukan semua kemungkinan celah dan kelemahan sistem yang mungkin mengakibatkan hilangnya informasi, pendapatan, reputasi di tangan karyawan atau orang luar Organisasi.

Tujuan dari pengujian keamanan adalah untuk mengidentifikasi ancaman dalam sistem dan mengukur kerentanan potensial, sehingga sistem tidak berhenti berfungsi atau dieksploitasi. Ini juga membantu dalam mendeteksi semua risiko keamanan yang mungkin dalam sistem dan membantu pengembang dalam memperbaiki masalah ini melalui pengkodean.

Dalam tutorial ini, Anda akan belajar-

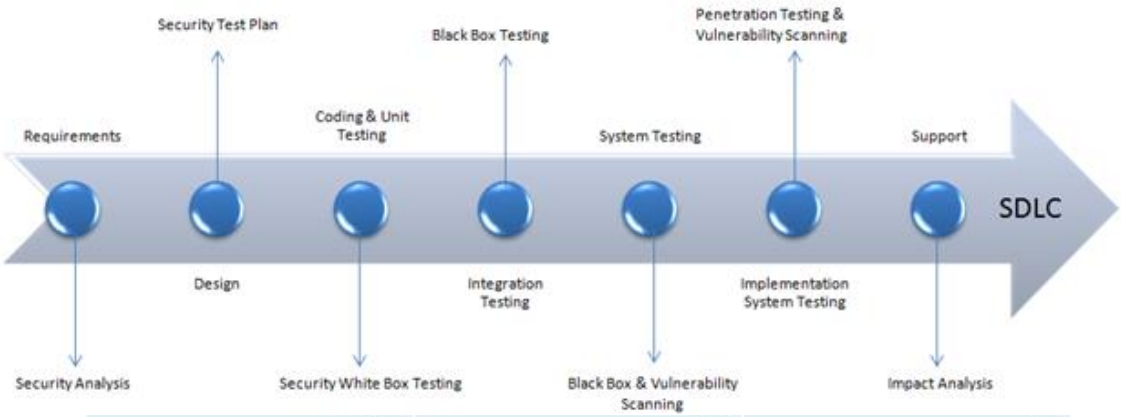
Apa itu Pengujian Keamanan?
Jenis Pengujian Keamanan
Bagaimana cara melakukan Pengujian Keamanan
Contoh Skenario Pengujian untuk Pengujian Keamanan
Metodologi / Pendekatan / Teknik untuk Pengujian Keamanan
Peran Pengujian Keamanan
Mitos dan Fakta Pengujian Keamanan
Jenis Pengujian Keamanan:
Ada tujuh jenis utama pengujian keamanan sesuai dengan manual metodologi Pengujian Keamanan Sumber Terbuka. Mereka dijelaskan sebagai berikut:



Pemindaian Kerentanan : Ini dilakukan melalui perangkat lunak otomatis untuk memindai sistem terhadap tanda-tanda kerentanan yang diketahui.
Pemindaian Keamanan: Ini melibatkan mengidentifikasi kelemahan jaringan dan sistem, dan kemudian memberikan solusi untuk mengurangi risiko ini. Pemindaian ini dapat dilakukan untuk pemindaian Manual dan Otomatis.
Pengujian penetrasi : Pengujian semacam ini mensimulasikan serangan dari peretas jahat. Pengujian ini melibatkan analisis sistem tertentu untuk memeriksa potensi kerentanan terhadap upaya peretasan eksternal.
Penilaian Risiko: Pengujian ini melibatkan analisis risiko keamanan yang diamati dalam organisasi. Risiko diklasifikasikan sebagai Rendah, Sedang dan Tinggi. Pengujian ini merekomendasikan kontrol dan langkah-langkah untuk mengurangi risiko.
Audit Keamanan: Ini adalah inspeksi internal Aplikasi dan sistem Operasi untuk kelemahan keamanan. Audit juga dapat dilakukan melalui inspeksi kode baris per baris
Peretasan etis: Meretas sistem Perangkat Lunak Organisasi. Tidak seperti peretas jahat, yang mencuri demi keuntungan mereka sendiri, tujuannya adalah untuk mengekspos kelemahan keamanan dalam sistem.
Penilaian Postur: Ini menggabungkan pemindaian Keamanan, Peretasan Etis dan Penilaian Risiko untuk menunjukkan postur keamanan keseluruhan organisasi.

Bagaimana cara melakukan Pengujian Keamanan
Selalu disetujui, bahwa biaya akan lebih banyak jika kita menunda pengujian keamanan setelah fase implementasi perangkat lunak atau setelah penyebaran. Jadi, perlu untuk melibatkan pengujian keamanan dalam siklus hidup SDLC pada fase sebelumnya.

Mari kita lihat proses Keamanan yang sesuai untuk diadopsi untuk setiap fase di SDLC



Fase SDLC	Proses Keamanan
Persyaratan	Analisis keamanan untuk persyaratan dan memeriksa kasus penyalahgunaan / penyalahgunaan
Desain	Analisis risiko keamanan untuk desain. Pengembangan Rencana Tes termasuk tes keamanan
Pengkodean dan Pengujian Unit	Pengujian Statis dan Dinamis dan Keamanan Pengujian Kotak Putih
Tes integrasi	Pengujian Kotak Hitam
Pengujian Sistem	Pengujian Kotak Hitam dan pemindaian Kerentanan
Pelaksanaan	Pengujian Penetrasi , Pemindaian Kerentanan
Mendukung	Analisis dampak Patch

https://www.cyberarmy.id

Bugcrowd

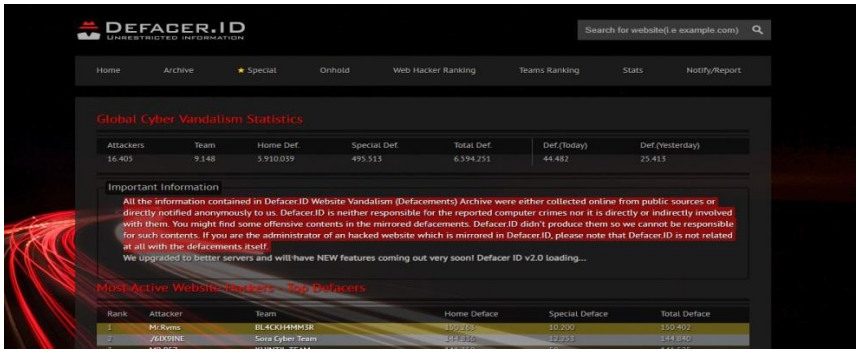
Bugcrowd is the #1 crowdsourced security platform. We prioritize our customers' operational efficiency, enabling them to reduce risk and release secure products to market faster. By combining the largest, most experienced triage team with the most skilled and trusted hackers around the world, Bugcrowd surfaces more, critical vulnerabilities — without hidden fees.

CVE Mitre

Dirty Cow

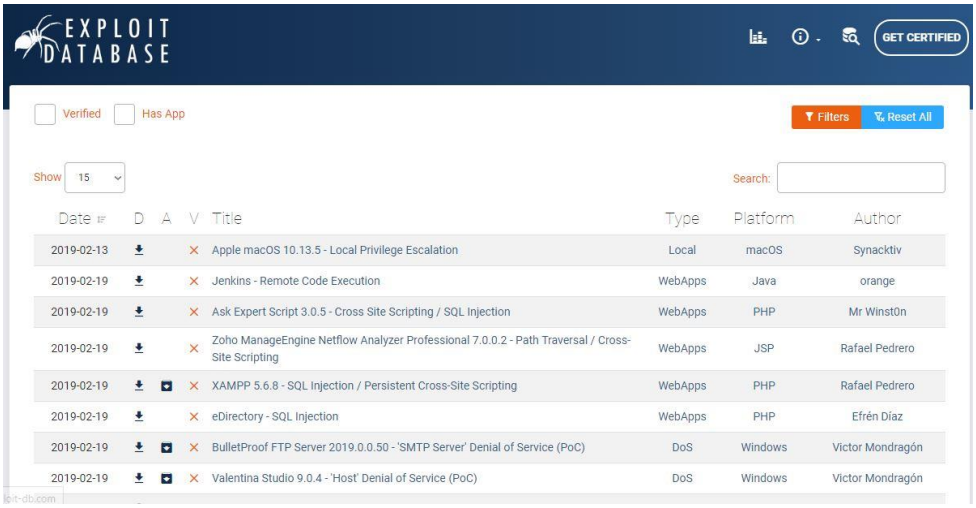
Dirty COW adalah kerentanan keamanan komputer untuk kernel Linux yang mempengaruhi semua sistem operasi berbasis Linux termasuk Android. Ini adalah bug eskalasi hak istimewa lokal yang mengeksploitasi kondisi ras dalam implementasi mekanisme copy-on-write dalam subsistem manajemen memori kernel.

Defacer.ID



Semua informasi yang terkandung dalam Arsip Vandalisme (Defacements) Situs Defacer.ID dikumpulkan secara online dari sumber-sumber publik atau secara langsung diberitahukan secara anonim kepada kami. Defacer.ID tidak bertanggung jawab atas kejahatan komputer yang dilaporkan atau terlibat langsung atau tidak langsung dengan kejahatan tersebut. Anda mungkin menemukan beberapa konten ofensif di defacements cermin. Defacer.ID tidak memproduksinya sehingga kami tidak dapat bertanggung jawab atas konten tersebut. Jika Anda adalah administrator situs web yang diretas yang dicerminkan dalam Defacer.ID, harap perhatikan bahwa Defacer.ID sama sekali tidak terkait dengan defacements itu sendiri.

Exploit.db



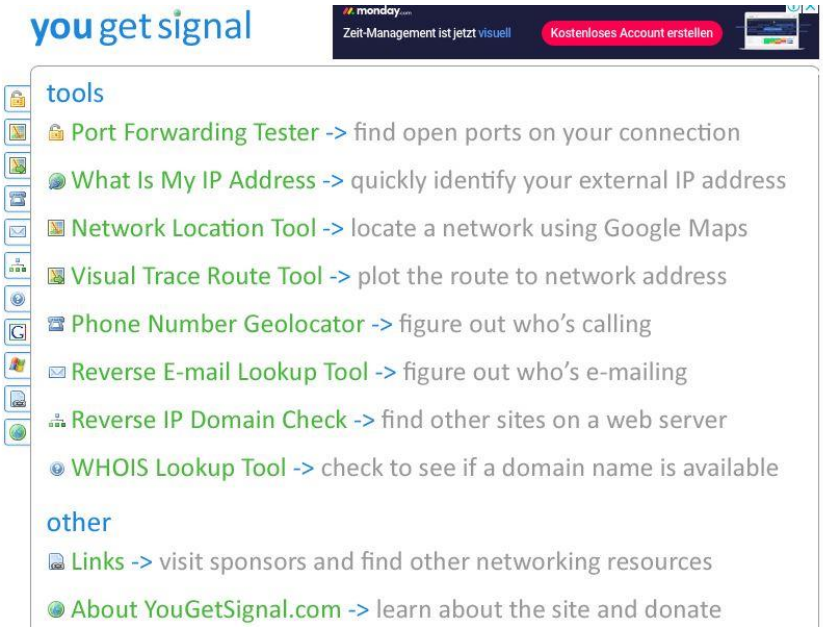
www.first.org

Sistem Penilaian Kerentanan Umum (Common Vulnerability Scoring System - CVSS) menyediakan cara untuk menangkap karakteristik utama kerentanan dan menghasilkan

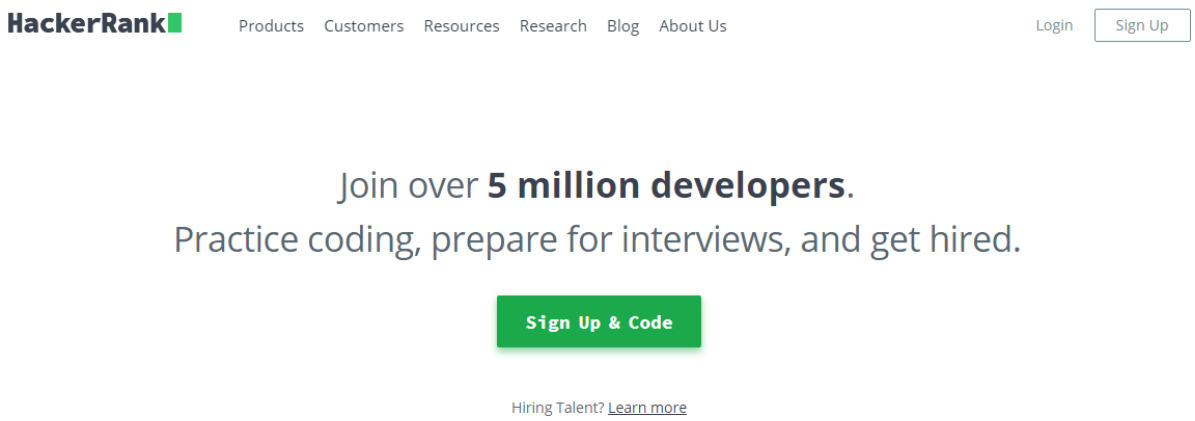
skor numerik yang mencerminkan tingkat keparahannya. Skor numerik kemudian dapat diterjemahkan ke dalam representasi kualitatif (seperti rendah, sedang, tinggi, dan kritis) untuk membantu organisasi menilai dengan benar dan memprioritaskan proses manajemen kerentanan mereka.

CVSS adalah standar yang diterbitkan yang digunakan oleh organisasi di seluruh dunia, dan misi SIG adalah untuk terus meningkatkannya.

https://www.yougetsignal.com



https://www.hackerrank.com



https://hackerone.com/bug-bounty-programs