Nama : Gonewaje
NIM : 09011181419005

Scanning Target using Most Popular Tools

Kali Linux merupakan distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan banyak digunakan untuk tujuan penetration testing, yang dipelihara dan didanai oleh Offensive Security. Kali linux sudah menyediakan berbagai macam tools yang dapat digunakan untuk keperluan penetration testing beberapa contohnya seperti exploit tools, forensic, reporting tools, man in the middle dan masih banyak lagi, kali linux merupakan distro linux dengan peringkat nomor 1 versi infosec institute untuk distro ethical hacking and penetration testing.

Salah satu tools yang ada pada kali linux adalah Nmap (Network mapper), 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.

Pada percobaan kali ini akan dilakukan tahap scanning/data collection terhadap target dimana target yang telah ditentukan adalah website Universitas Sriwijaya (http://www.unsri.ac.id), scanning akan melalui beberapa tahapan seperti :

Nama : Gonewaje
NIM : 09011181419005

1. Scanning System

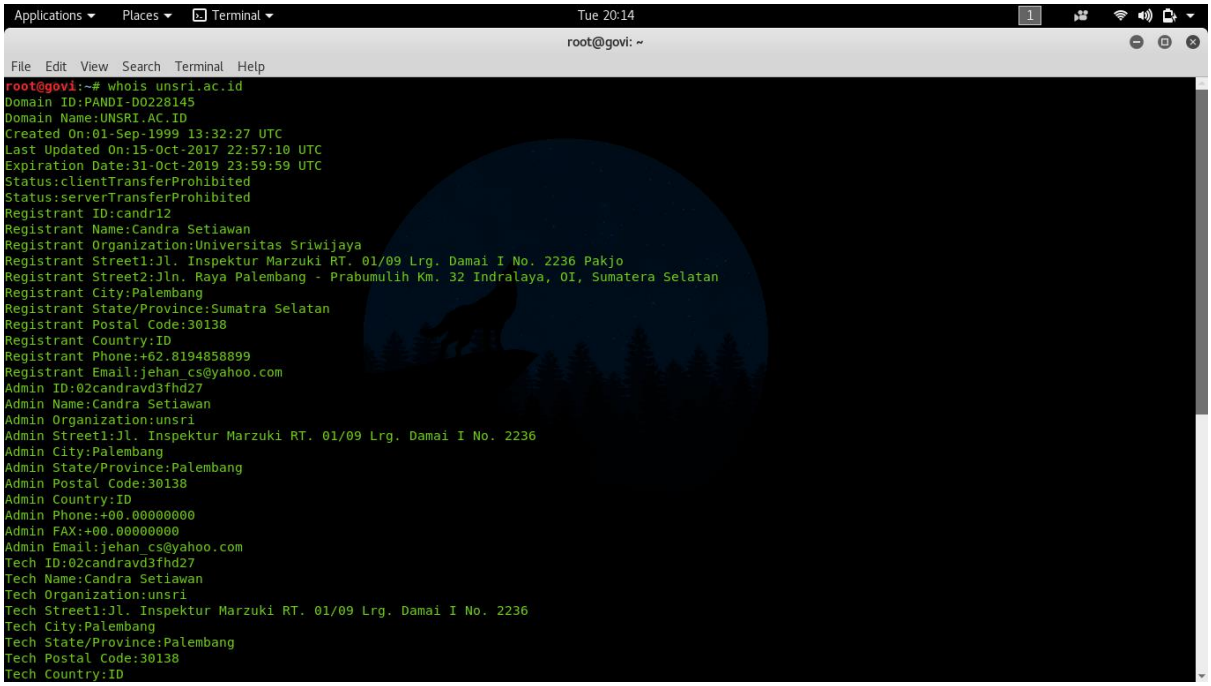
2. Scanning Network

3. Scanning Open Port

4.Scanning Operation System (OS)

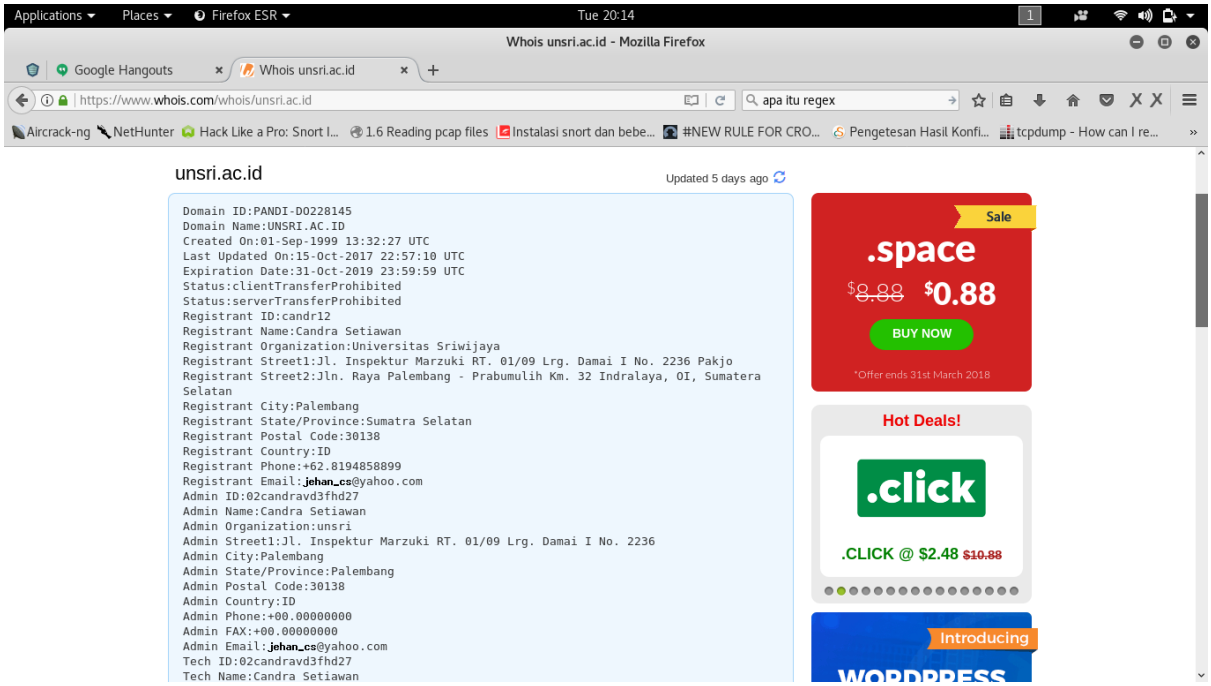
Pada tahap scanning atau data collection ini akan menggunakan salah satu tools yang ada pada kali linux yaitu Nmap serta beberapa website tambahan yang berguna untuk tahapan ini.

Langkah pertama yang dilakukan adalah melakukan pencarian informasi tentang website target, disini digunakan whois dapat menggunakan versi console ataupun melalui website.



Tampilan whois versi console

Nama : Gonewaje
NIM : 09011181419005

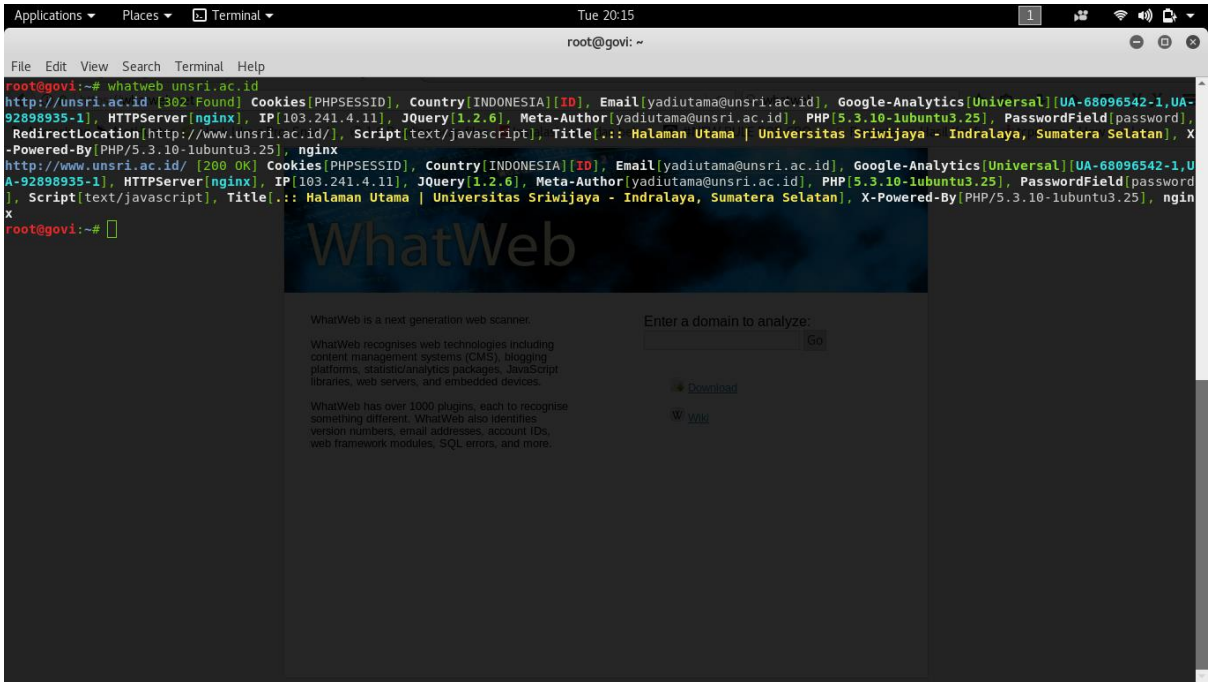


Tampilan whois versi website

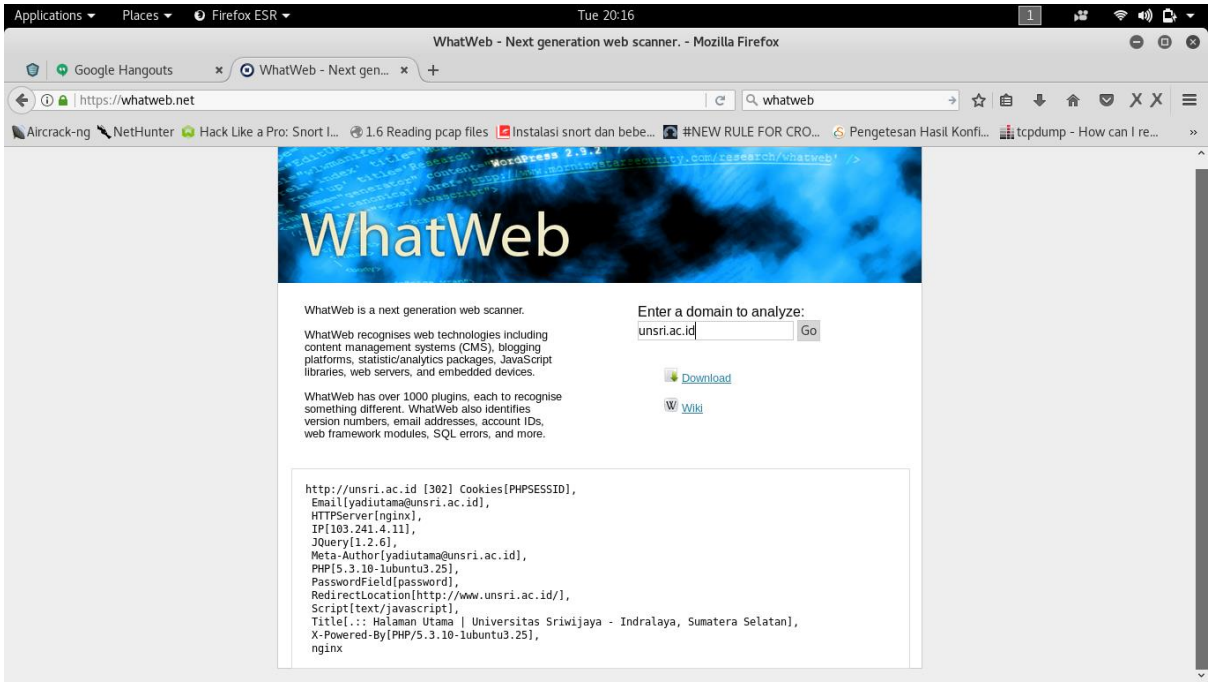
Secara keseluruhan tidak ada yang berbeda dari whois versi console ataupun website karena memang berasal dari satu sumber. Dengan menggunakan whois kita dapat mengetahui informasi seputar domain yang didaftarkan target seperti Domain-ID target, kapan website target dibuat dan kapan expiration date dari domain target, Nama pendaftar domain target, Alamat lengkap pendaftar domain target, telepon, email dan lain sebagainya. Sebagai contoh sederhana adalah dari informasi yang didapatkan menggunakan whois, salah satunya memanfaatkan nama pendaftar domain, dengan bermodalkan nama pendaftar seorang hacker dapat melakukan kejahatan berbahaya seperti meneror target, mendapatkan informasi penting melalui sosial media (tanggal lahir, nama anak, istri/suami, hobi,dll) yang dapat dimanfaatkan untuk tindakan lainnya.

Langkah selanjutnya selain menggunakan whois adalah menggunakan whatweb, whatweb juga tersedia dalam dua versi yaitu console dan web

Nama : Gonewaje
NIM : 09011181419005



Tampilan whatweb versi console



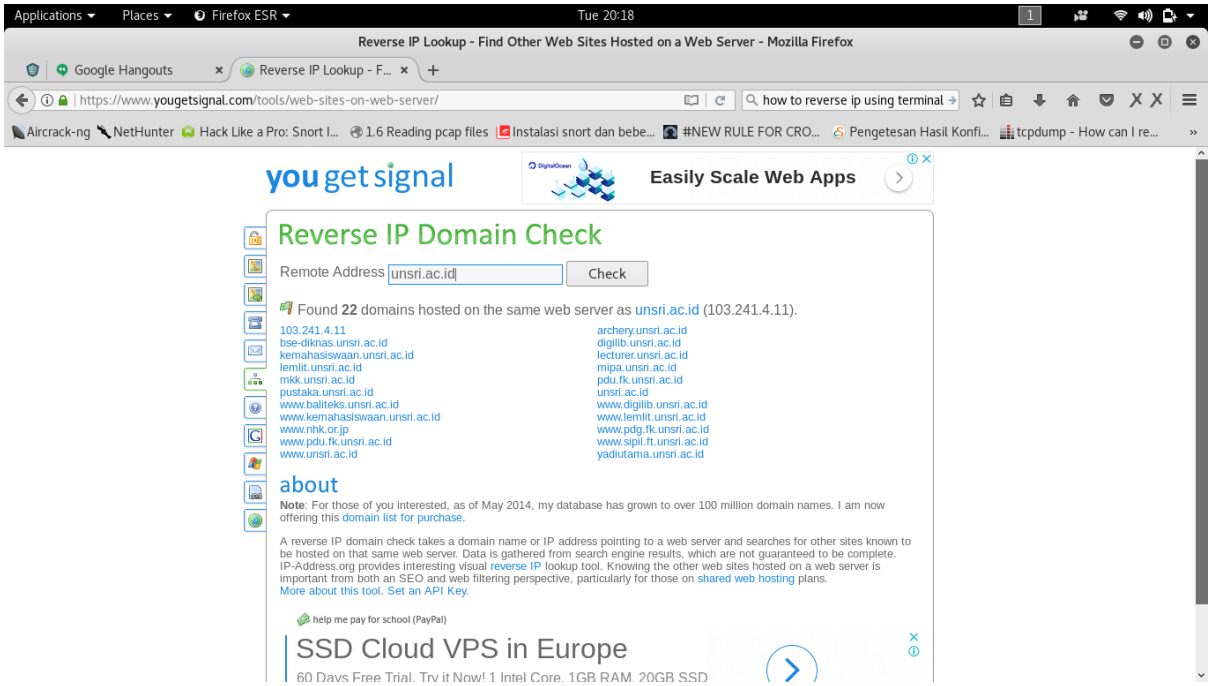
Tampilan wahtweb versi web

Whatweb berbeda dengan whois yang menampilkan informasi mengenai domain target, whatweb lebih kepada dengan apa target tersebut “dibangun”, misalkan target dibangun dengan server nginx, ip target adalah 103.241.4.11, PHP menggunakan lubuntu dan sebagainya. Dari salah satu field tersebut misalkan server yang digunakan target adalah nginx makan dapat digunakan untuk mencari CVE dari nginx itu sendiri. CVE merupakan Common Vulnerabiliti Exposure dimana merupakan kumpulan vulnerabiliti dari sistem yang ada pada

Nama : Gonewaje
NIM : 09011181419005

saat ini, CVE dapat digunakan untuk ‘merusak’ target tergantung dari administrator target itu sendiri dalam melakukan update informasi mengenai CVE sistem yang mereka gunakan.

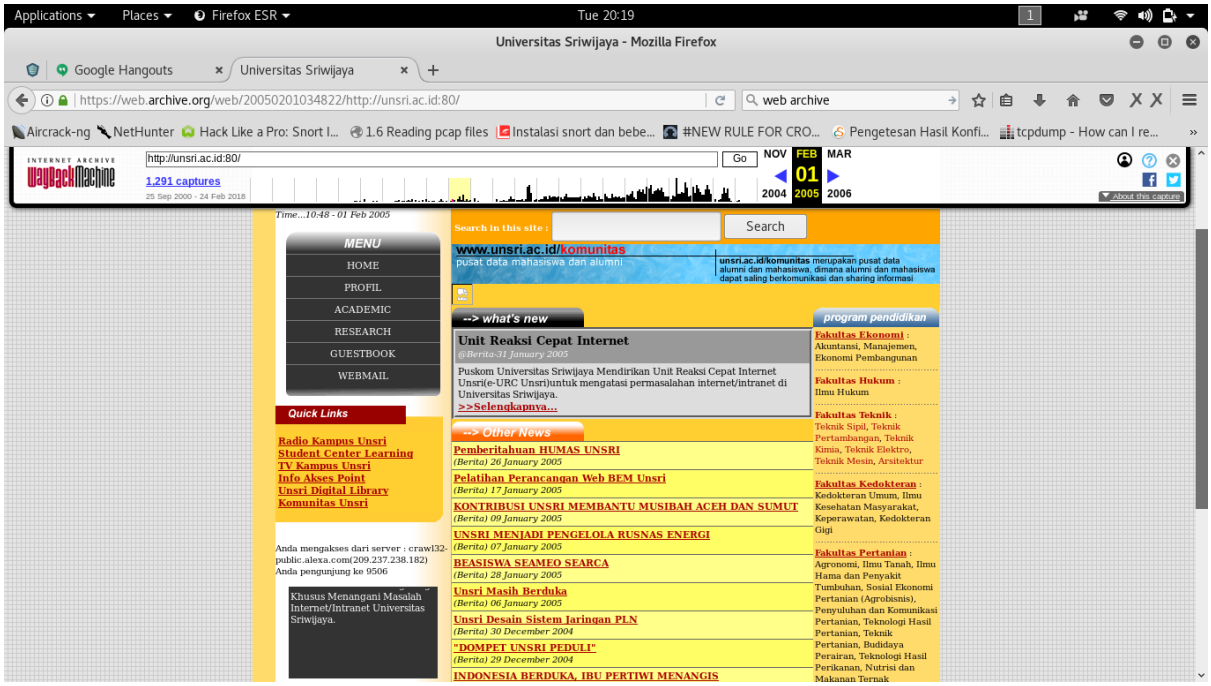
Kemudian yang dapat dilakukan setelah scanning menggunakan whatweb, kita dapat pula melakukan scanning terhadap domain apa saja yang terkait dengan si target menggunakan Reverse IP.



Contoh penggunakan reverse ip oleh para hacker adalah, hacker dapat menggunakan daftar domain yang terhubung kepada satu domain pusat atau website pusat yang target kehendaki untuk mengambil alih salah satu ataupun seluruh sistem. Misalkan, website utama target adalah unsri.ac.id dan memiliki reverse ip domain seperti pada gambar diatas, ternyata sang hacker mendapatkan celah pada website pustaka.unsri.ac.id dan berhasil mendapatkan akses root, dari situ bukan tidak mungkin apabila hacker dapat mengambil alih website utama target atau bahkan seluruh website yang memiliki satu domain terhadap website utama target.

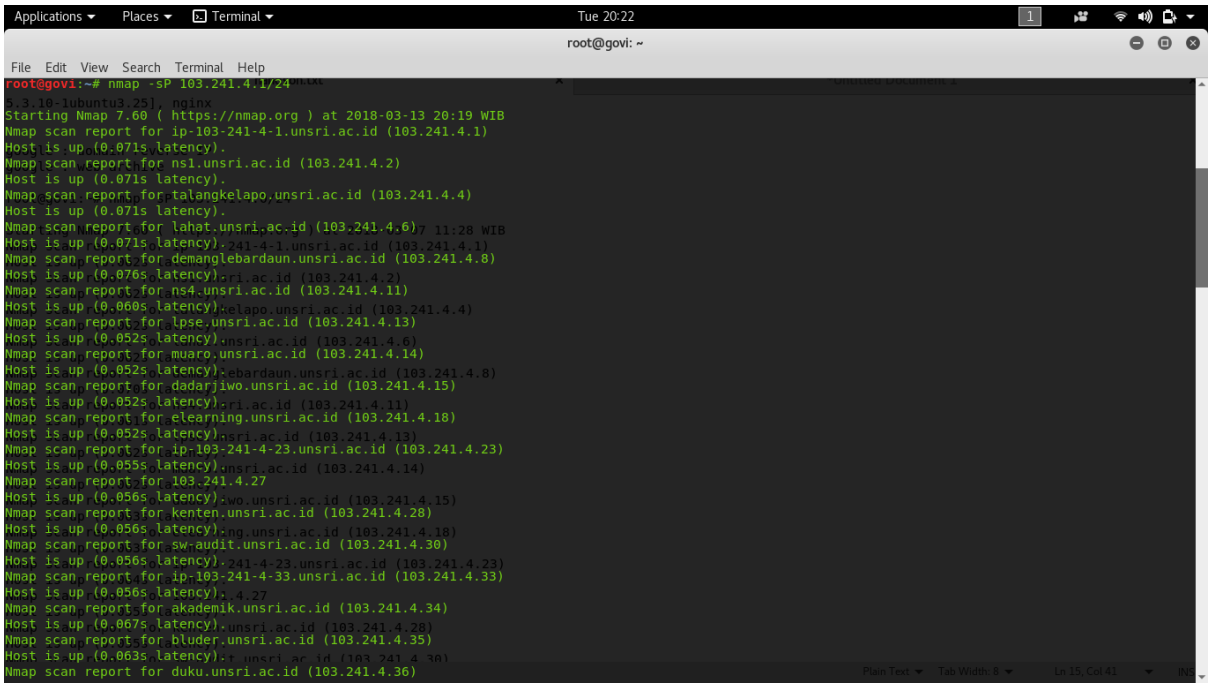
Sebelum menggunakan nmap untuk melakukan scanning lebih lanjut, mungkin informasi tambahan ini dapat digunakan untuk suatu kepentingan kedepannya. Website yang berguna lainnya disisi defense adalah web archive, web archive adalah sebuah website yang mengumpulkan beberapa arsip website yang berhasil disnapshot oleh website itu sendiri, contoh pada website unsri apabila dilihar arsipnya maka yang berhasil disnapshot dimulai pada tahun 2000 dan berikut contoh salah satu snapshot pada tanggal 1 februari 2005

Nama : Gonewaje
NIM : 09011181419005



Web arsip ini dapat digunakan untuk mengetahui informasi-informasi terdahulu yang mungkin terlewatkan oleh administrator atau dapat pula digunakan sebagai tambahan informasi apabila terjadi serangan hacker atau bahkan dapat digunakan oleh hacker itu sendiri.

Scanning selanjutnya adalah menggunakan nmap dan melakukan scanning terhadap host ip target

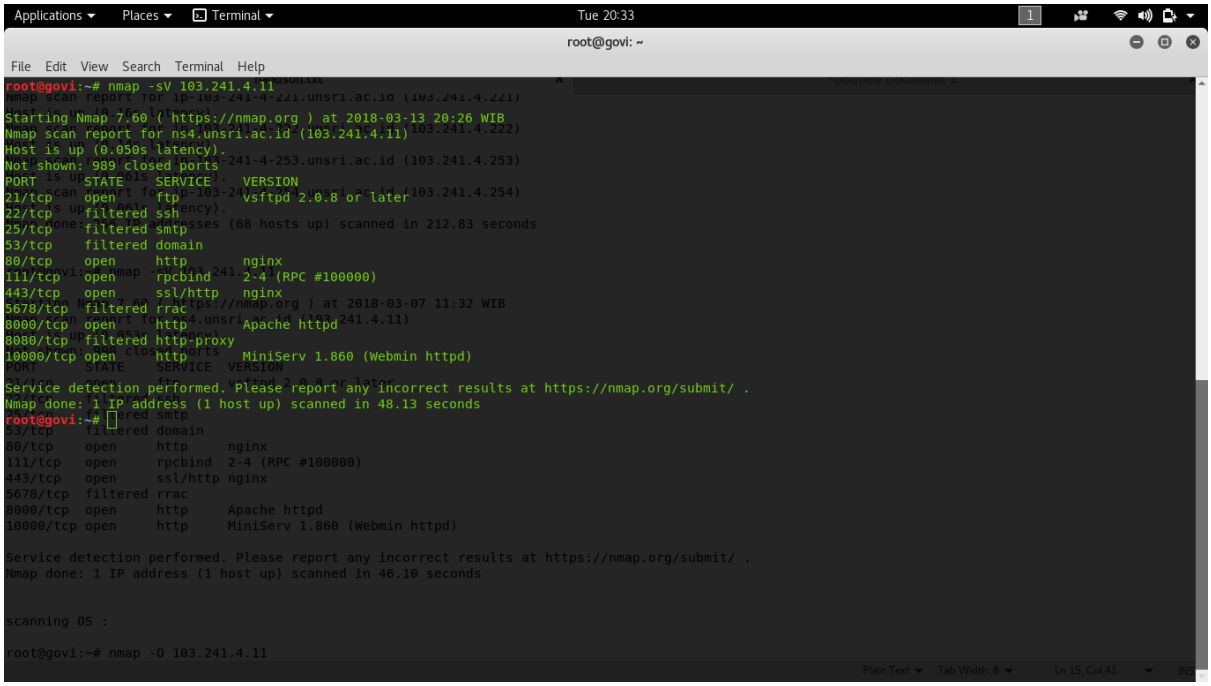


Dilakukan scanning terhadap host ip target dari range 103.241.4.1-103.241.4.255, didapatkan hasil bahwa beberapa host tersebut memiliki beberapa domain aktif dan beberapa domain

Nama : Gonewaje
NIM : 09011181419005

yang telah direverse contohnya domain duku.unsri.ac.id yang direverse menjadi domain suliet.unsri.ac.id

Scanning selanjutnya dengan nmap yang dilakukan adalah scanning open port



Scanning open port dilakukan untuk mengetahui port-port mana saja yang terbuka dan dimungkinkan oleh para hacker untuk masuk kedalam sistem target, contoh adalah port 22 dengan service ssh memiliki status filtered yang berarti tidak sembarang user dapat menggunakan port tersebut, contoh port yang terbuka adalah port 10000 dengan protokol tcp dan service http digunakan untuk webmin atau untuk administrasi sistem berbasis unix.

Terakhir adalah melakukan scanning OS, scanning ini dapat dimanfaatkan untuk mengetahui OS apa yang digunakan oleh target dan dapat diketahui hole dari OS tersebut menggunakan CVE dari OS itu sendiri, hal ini juga tergantung kepada administrator dari target apakah update terhadap CVE OS yang mereka gunakan atau tidak.

Nama : Gonewaje
NIM : 09011181419005