TUGAS KEAMANAN JARINGAN

NAMA: SAROS SAKIYANA

NIM: 09011181320038

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

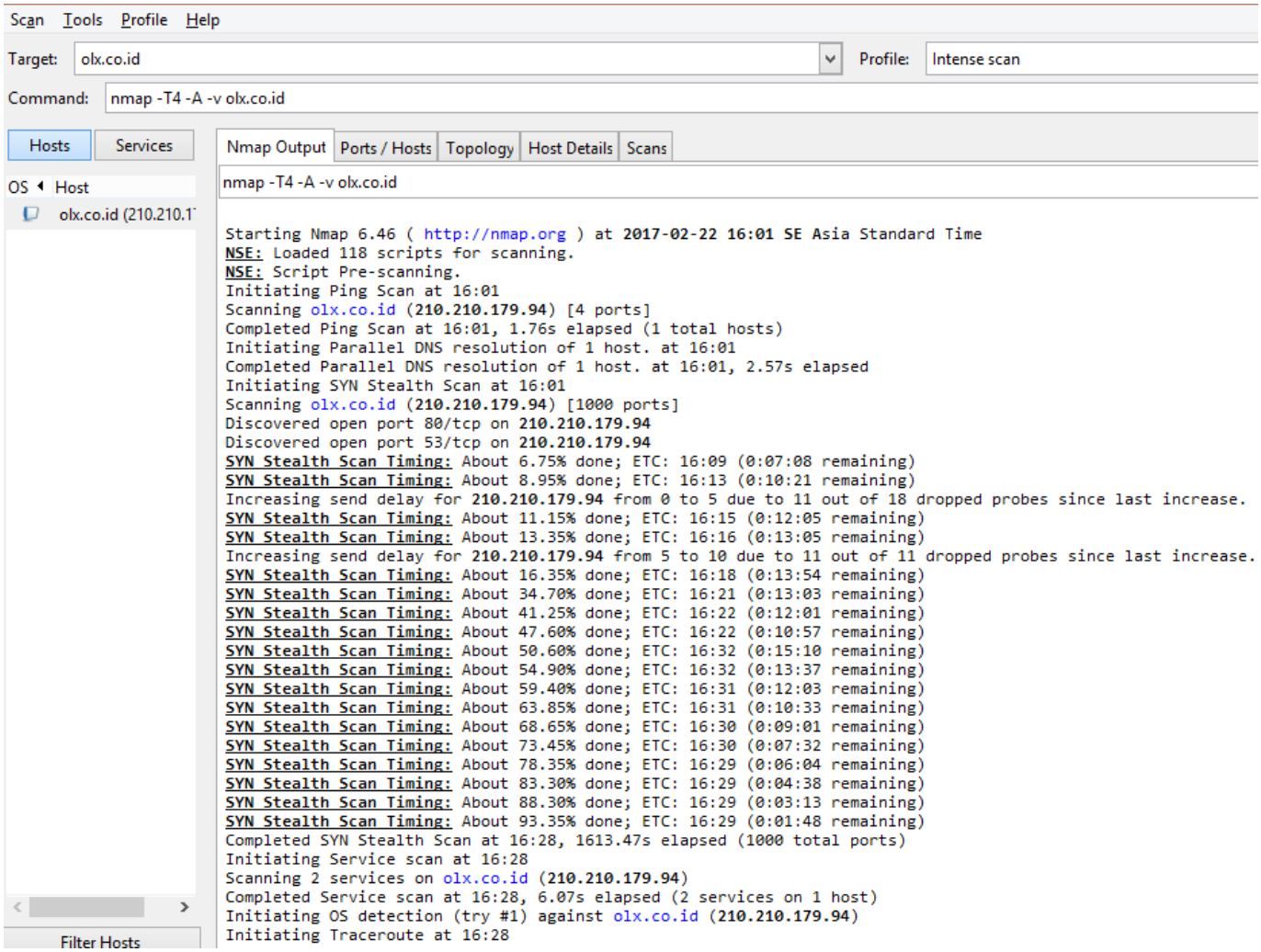
2017

SCANNING menggunakan ZenMap:

Dengan nama domain: olx.co.id

Nama output:

Nmap mencetak output interaktif ke stdout seperti biasa. Pada perintah **olx.co.id** mencetak xml ke co.id dan mengisi seluruh output standart dengan hasill interaktif yang sama yang akan ditampilkan gambar dibawah ini:



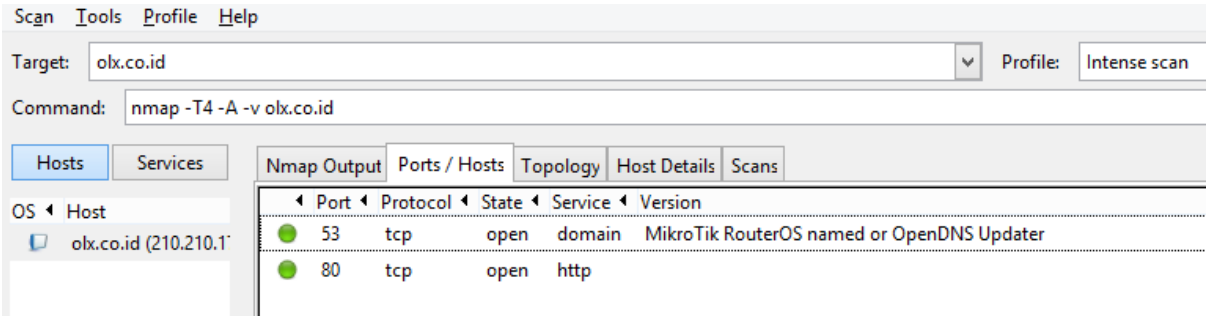
```
Completed Traceroute at 16:29, 10.30s elapsed
NSE: Script scanning 210.210.179.94.
Initiating NSE at 16:29
NSE Timing: About 66.67% done; ETC: 16:30 (0:00:30 remaining)
Completed NSE at 16:32, 177.91s elapsed
Nmap scan report for olx.co.id (210.210.179.94)
Host is up (0.22s latency).
Other addresses for olx.co.id (not scanned): 210.210.179.104 210.210.179.84
rDNS record for 210.210.179.94: 210.210.179.94.cbn.net.id
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  MikroTik RouterOS named or OpenDNS Updater
80/tcp open  http?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linksys Linux 2.4.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linksys:linux_kernel:2.4 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 80/tcp)
HOP RTT    ADDRESS
1   ... 30

NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1835.86 seconds
           Raw packets sent: 2353 (106.516KB) | Rcvd: 405 (44.848KB)
```

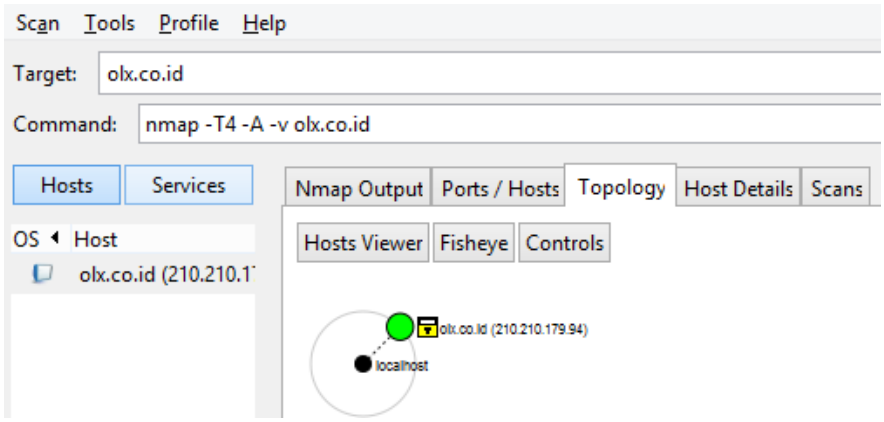
Ports/host:

Port/host pada domain olx.co.id, memiliki port 53 dan 80 dan menggunakan protokol tcp. Port scanning adalah proses koneksi keport port tcp pada host yang menjadi target untuk menentukan service apa yang sedang berjalan. Dengan mengidentifikasi port-port yang listenng ini kita dapat menetukan jenis aplikasi dan sistem operasi yang digunakan pada hots tersebut.



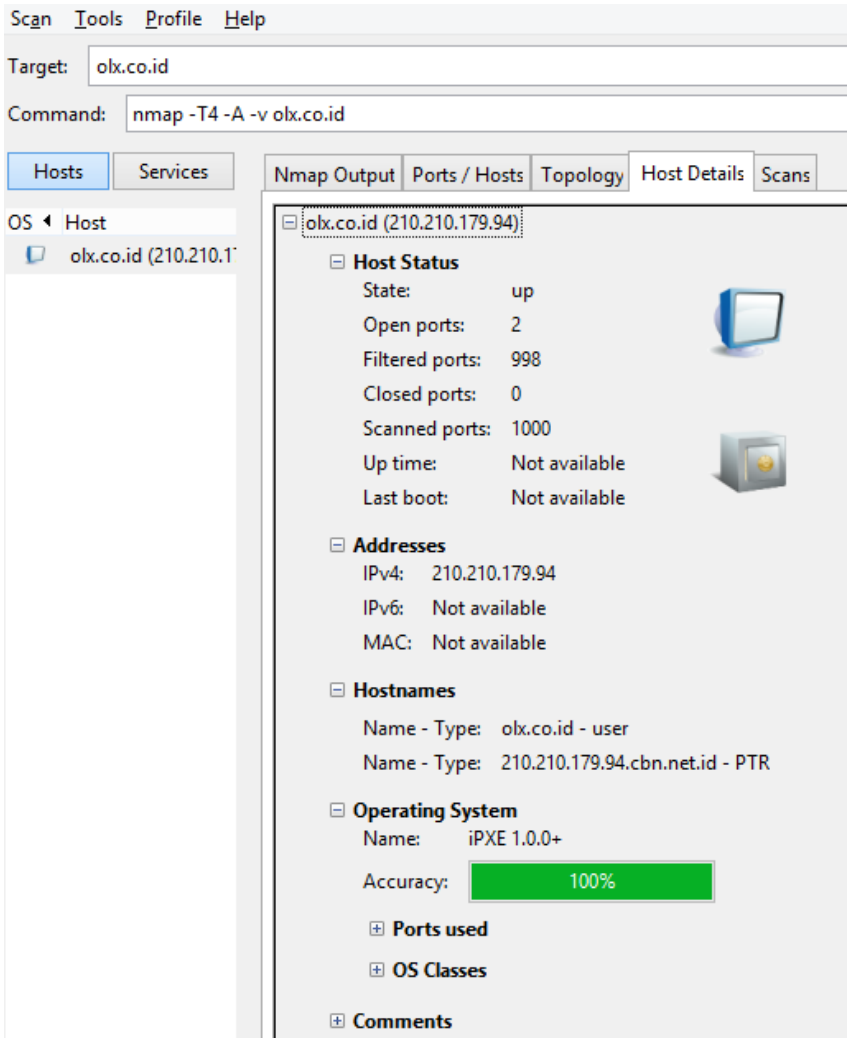
Topology:

Pada gambar topoloy terdapat ip olx.co.id (210.210.179.94)



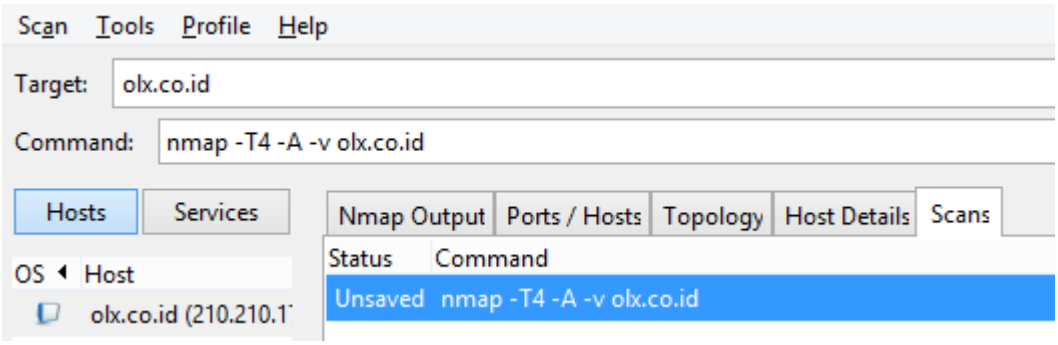
Host details:

Pada host detail pada domain olx.co.id terdapat host status, addresses, hostname, operating sistem pada operating sistem ini memiliki accurasy 100 %



Scans:

Pada scans terdapat status command: unsaved nmap –T4-A-v olx.co.i



Analisa:

Dari hasil scanning diatas dapat kita analisa informasi-informasi yang berguna untuk proses hacking. Informasi-informasi tersebut adalah: nama web target, ip address, status server, os yang digunakan dan port yang ada pada domain yang kita cari misal olx.co.id

Zenmap adalah aplikasi multi platform sebagai interface sederhana untuk aplikasi nmap. Fungsi zenmap itu sendiri adalah untuk eksplorasi dan audit keamanan jaringan dan memeriksa jaringan besar secara cepat, meskipun ia zenmap dapat pula bekerja terhadap host tunggal.

Kesimpulan:

Hasil percobaan diatas telah melakukan scanning pada suatu host, scannning merupakan salah satu langkah yang dasar dalam memetahkan jaringan. Untuk menentukan apakah sistem tersebut masih hidup, dan alat yang digunakan untuk melakukan pemetaan tersebut adalah zenmap.

http://cve.mitre.org/cgibin/cvekey.cgi?keyword=domain++MikroTik+RouterOS+named+or+OpenDNS+Updater

CVE:

Search Results

There are **69** CVE entries that match your search.

Name	Description
CVE-2013-2890	drivers/hid/hid-sony.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SONY is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.
CVE-2011-3590	The Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, includes all of root's SSH private keys within a vmcore file, which allows context-dependent attackers to obtain sensitive information by inspecting the file content.
CVE-2011-3589	The Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, uses world-readable permissions for vmcore files, which allows local users to obtain sensitive information by inspecting the file content, as demonstrated by a search for a root SSH key.
CVE-2011-3588	The SSH configuration in the Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, disables the StrictHostKeyChecking option, which allows man-in-the-middle attackers to spoof kdump servers, and obtain sensitive core information, by using an arbitrary SSH key.
CVE-2011-1126	VMware vmrun, as used in VIX API 1.x before 1.10.3 and VMware Workstation 6.5.x and 7.x before 7.1.4 build 385536 on Linux, might allow local users to gain privileges via a Trojan horse shared library in an unspecified directory.
CVE-2011-0627	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.
CVE-2011-0611	Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content; as demonstrated by a Microsoft Office document with an embedded .swf file that has a size inconsistency in a "group of included constants," object type confusion, ActionScript that adds custom functions to prototypes, and Date objects; and as exploited in the wild in April 2011.
CVE-2011-0609	Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris; 10.1.106.16 and earlier on Android; Adobe AIR 2.5.1 and earlier; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader and Acrobat 9.x through 9.4.2 and 10.x through 10.0.1 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content, as demonstrated by a .swf file embedded in an Excel spreadsheet, and as exploited in the wild in March 2011.
CVE-2010-1507	WebYaST in yast2-webclient in SUSE Linux Enterprise (SLE) 11 on the WebYaST appliance uses a fixed secret key that is embedded in the appliance's image, which allows remote attackers to spoof session cookies by leveraging knowledge of this key.
CVE-2009-3733	Directory traversal vulnerability in VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138 on Linux, VMware ESXi 3.5, and VMware ESX 3.0.3 and 3.5 allows remote attackers to read arbitrary files via unspecified vectors.
CVE-2009-3228	The tc_fill_tclass function in net/sched/sch_api.c in the tc subsystem in the Linux kernel 2.4.x before 2.4.37.6 and 2.6.x before 2.6.31-rc9 does not initialize certain (1) tcm__pad1 and (2) tcm__pad2 structure members, which might allow local users to obtain sensitive information from kernel memory via unspecified vectors.
CVE-2009-2903	Memory leak in the appletalk subsystem in the Linux kernel 2.4.x through 2.4.37.6 and 2.6.x through 2.6.31, when the appletalk and ipddp modules are loaded but the ipddp"N" device is not found, allows remote attackers to cause a denial of service (memory consumption) via IP-DDP datagrams.
CVE-2009-0396	The Sony Ericsson W910i, W660i, K618i, K610i, Z610i, K810i, K660i, W880i, and K530i phones allow remote attackers to cause a denial of service (device reboot or hang-up) via a malformed WAP Push packet to (1) SMS or (2) UDP port 2948.
CVE-2008-0967	Untrusted search path vulnerability in vmware-authd in VMware Workstation 5.x before 5.5.7 build 91707 and 6.x before 6.0.4 build 93057, VMware Player 1.x before 1.0.7 build 91707 and 2.x before 2.0.4 build 93057, and VMware Server before 1.0.6 build 91891 on Linux, and VMware ESXi 3.5 and VMware ESX 2.5.4 through 3.5, allows local users to gain privileges via a library path option in a configuration file.
CVE-2007-6206	The do_coredump function in fs/exec.c in Linux kernel 2.4.x and 2.6.x up to 2.6.24-rc3, and possibly other versions, does not change the UID of a core dump file if it exists before a root process creates a core dump in the same location, which might allow local users to obtain sensitive information.
CVE-2007-5208	hpssd in Hewlett-Packard Linux Imaging and Printing Project (hplip) 1.x and 2.x before 2.7.10 allows context-dependent attackers to execute arbitrary commands via shell metacharacters in a from address, which is not properly handled when invoking sendmail.
CVE-2007-4573	The IA32 system call emulation functionality in Linux kernel 2.4.x and 2.6.x before 2.6.22.7, when running on the x86_64 architecture, does not zero extend the eax register after the 32bit entry path to ptrace is used, which might allow local users to gain privileges by triggering an out-of-bounds access to the system call table using the %RAX register.

CVE-2003-0552	Linux 2.4.x allows remote attackers to spoof the bridge Forwarding table via forged packets whose source addresses are the same as the target.
CVE-2003-0551	The STP protocol implementation in Linux 2.4.x does not properly verify certain lengths, which could allow attackers to cause a denial of service.
CVE-2003-0550	The STP protocol, as enabled in Linux 2.4.x, does not provide sufficient security by design, which allows attackers to modify the bridge topology.
CVE-2003-0476	The execve system call in Linux 2.4.x records the file descriptor of the executable process in the file table of the calling process, which allows local users to gain read access to restricted file descriptors.
CVE-2003-0461	/proc/tty/driver/serial in Linux 2.4.x reveals the exact number of characters used in serial links, which could allow local users to obtain potentially sensitive information such as the length of passwords.
CVE-2003-0127	The kernel module loader in Linux kernel 2.2.x before 2.2.25, and 2.4.x before 2.4.21, allows local users to gain root privileges by using ptrace to attach to a child process that is spawned by the kernel.
CVE-2002-1865	Buffer overflow in the Embedded HTTP server, as used in (1) D-Link DI-804 4.68, Dl-704 V2.56b6, and Dl-704 V2.56b5 and (2) Linksys Etherfast BEFW11S4 Wireless AP + Cable/DSL Router 1.37.2 through 1.42.7 and Linksys WAP11 1.3 and 1.4, allows remote attackers to cause a denial of service (crash) via a long header, as demonstrated using the Host header.
CVE-2002-0510	The UDP implementation in Linux 2.4.x kernels keeps the IP Identification field at 0 for all non-fragmented packets, which could allow remote attackers to determine that a target system is running Linux.
CVE-2002-0060	IRC connection tracking helper module in the netfilter subsystem for Linux 2.4.18-pre9 and earlier does not properly set the mask for conntrack expectations for incoming DCC connections, which could allow remote attackers to bypass intended firewall restrictions.
CVE-2001-1384	ptrace in Linux 2.2.x through 2.2.19, and 2.4.x through 2.4.9, allows local users to gain root privileges by running ptrace on a setuid or setgid program that itself calls an unprivileged program, such as newgrp.
CVE-2000-0727	xpdf PDF viewer client earlier than 0.91 does not properly launch a web browser for embedded URL's, which allows an attacker to execute arbitrary commands via a URL that contains shell metacharacters.
CVE-1999-0398	In some instances of SSH 1.2.27 and 2.0.11 on Linux systems, SSH will allow users with expired accounts to login.