TUGAS

KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : INDAH SARI

NIM : 09011181320011

JURUSAN SISTEM KOMPUTER

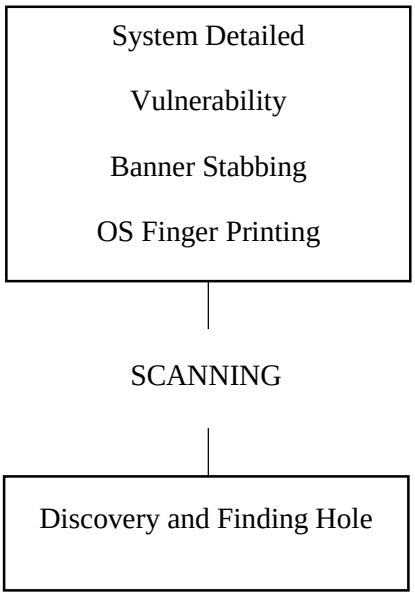
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017 – 2018

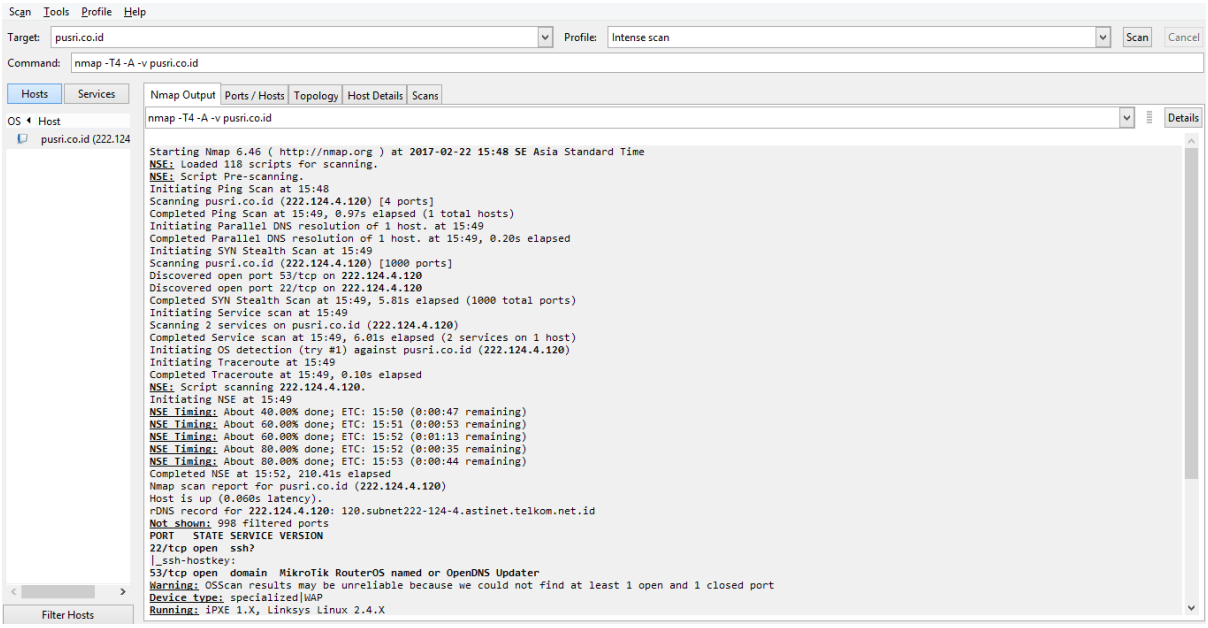
PERTANYAAN :

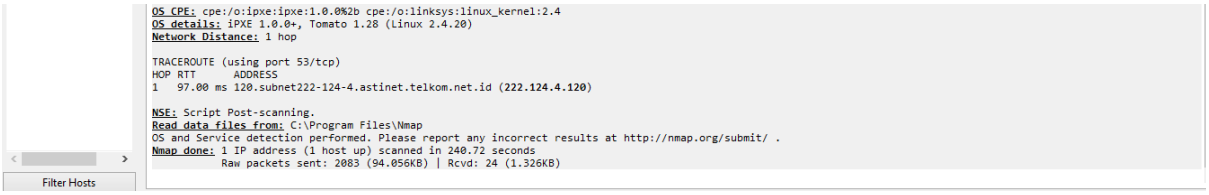
Lakukan SCANNING pada user/ target



JAWABAN :

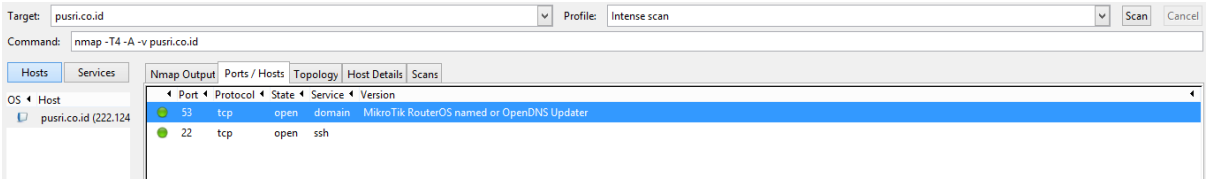
Hasil SCANNING dari domain pusri.co.id dengan menggunakan Zenmap





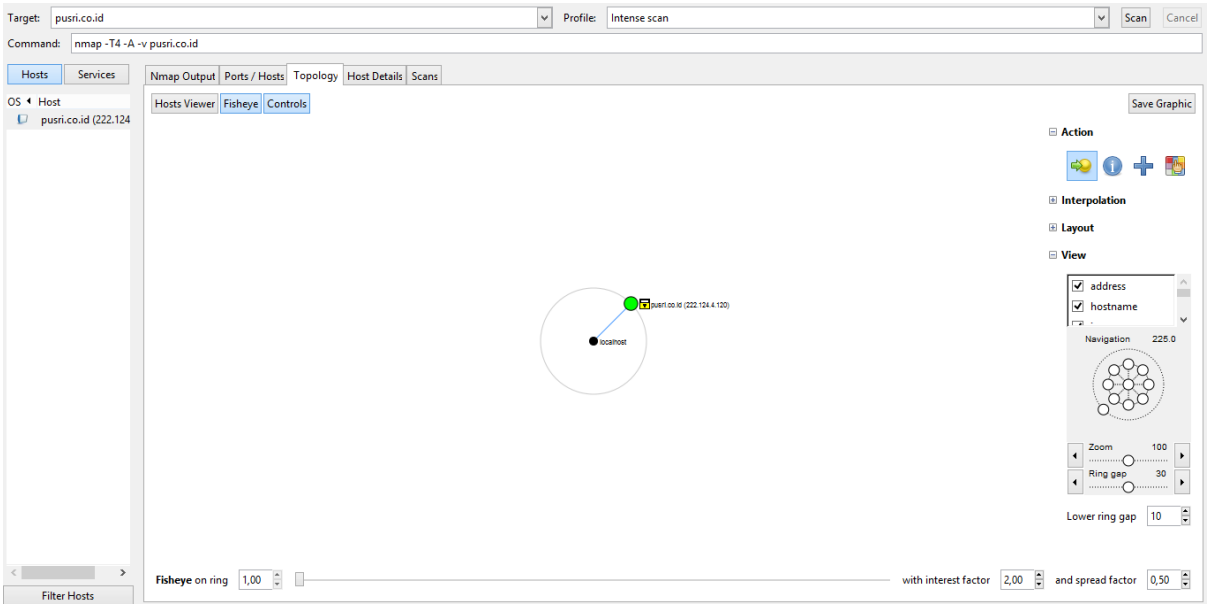
IP address dari domain ini adalah 222.124.4.120, Device type -nya menggunakan specialized |WAP, dan Running di iPXE 1.X, Linksys Linux 2.4. X, OS details: iPXE 1.0.0 +, Tomato 1.28 (Linux 2.4.20), dan memiliki satu hop dalam network distance

Port/ Host yang aktif dan layananannya



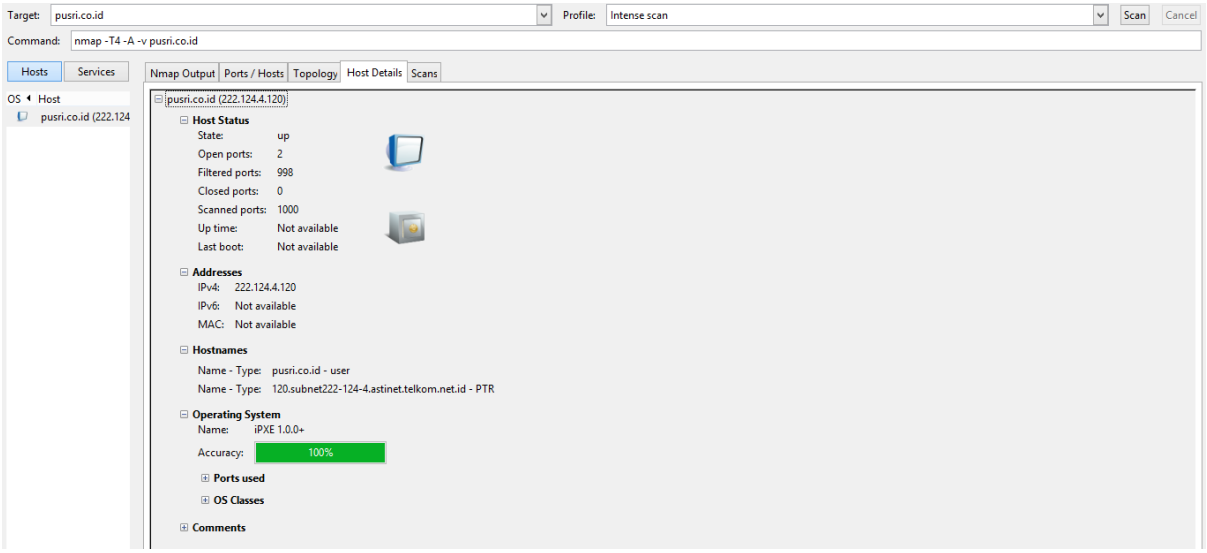
Pada gambar diatas dapat dilihat pusri.co.id memiliki dua layanan (service) yang aktif yaitu: domain yang versinya Mikrotik Router OS named or Open DNS Updater dan SSH. Dimana kedua layanan ini memakai Protocol TCP, port yang aktif di Mikrotik Router OS named or Open DNS Updater adalah PORT 53, sedangkan pada SSH port yang aktif adalah PORT 22

Topology pada domain pusri.co.id



Dapat dilihat dari gambar Topology diatas memiliki satu hop yang terhubung dari localhost ke pusri.co.id (222.124.4.120)

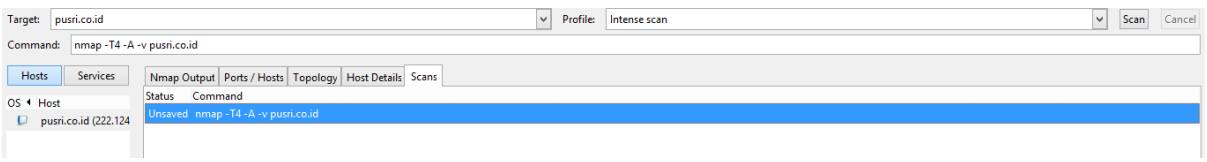
Host Details



Pada Host Detail menampilkan Host status, Addresses, Hostnames, Operating System, dan comments

- Pada host status: state –nya sedang UP, PORT yang tersedia ada dua, Filtered ports 998, Scanned ports 1000.
- Pada Addresses: IPv4 222.124.4.120, IPv6 not available, dan MAC not available
- Pada Hostnames ada dua yaitu: nama type pusri.co.id – user, dan 120.subnet222-124-4.astinet.telkom.net.id - PTR
- Pada Operating System: iPXE 1.0.0+, akurasinya 100%
- Pada comments: tidak menampilkan apa – apa

Scans



Pada gambar scans diatas dapat dilihat statusnya Unsave, dan command: nmap - T4 – A – v pusri.co.id

CVE

Mencari CVE dengan menggunakan Running: iPXE 1.X, Linksys Linux 2.4.X.

Dari iPXE 1.X memiliki 283 CVE (hanya sebagian yang ditampilkan)

Search Results

There are **283** CVE entries that match your search.

Name	Description
CVE-2017-6072	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via defaultadmin.
CVE-2017-6071	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to conduct information-disclosure attacks via exportxml.
CVE-2017-6070	CMS Made Simple version 1.x Form Builder before version 0.8.1.6 allows remote attackers to execute PHP code via the cntnt01fbrp_forma_form_template parameter in admin_store_form.
CVE-2017-5595	A file disclosure and inclusion vulnerability exists in web/views/file.php in ZoneMinder 1.x through v1.30.0 because of unfiltered user-input being passed to readfile(), which allows an authenticated attacker to read local system files (e.g., /etc/passwd) in the context of the web server user (www-data). The attack vector is a .. (dot dot) in the path parameter within a zm/index.php?view=file&path= request.
CVE-2016-9274	Untrusted search path vulnerability in Git 1.x for Windows allows local users to gain privileges via a Trojan horse git.exe file in the current working directory. NOTE: 2.x is unaffected.
CVE-2016-7954	Bundler 1.x might allow remote attackers to inject arbitrary Ruby code into an application by leveraging a gem name collision on a secondary source. NOTE: this might overlap CVE-2013-0334.
CVE-2016-7191	The Microsoft Azure Active Directory Passport (aka Passport-Azure-AD) library 1.x before 1.4.6 and 2.x before 2.0.1 for Node.js does not recognize the validateIssuer setting, which allows remote attackers to bypass authentication via a crafted token.
CVE-2016-5892	Cross-site scripting (XSS) vulnerability in IBM 10x, as used in Multi-Enterprise Integration Gateway 1.x through 1.0.0.1 and B2B Advanced Communications before 1.0.0.5_2, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.
CVE-2016-5540	Unspecified vulnerability in the Oracle Retail Xstore Payment component in Oracle Retail Applications 1.x allows local users to affect confidentiality and integrity via unknown vectors.
CVE-2016-5539	Unspecified vulnerability in the Oracle Retail Xstore Payment component in Oracle Retail Applications 1.x allows local users to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2016-5180	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly execute arbitrary code via a hostname with an escaped trailing dot.
CVE-2016-4526	ABB DataManagerPro 1.x before 1.7.1 allows local users to gain privileges by replacing a DLL file in the package directory.
CVE-2016-2784	CMS Made Simple 2.x before 2.1.3 and 1.x before 1.12.2, when Smarty Cache is activated, allow remote attackers to conduct cache poisoning attacks, modify links, and conduct cross-site scripting (XSS) attacks via a crafted HTTP Host header in a request.
CVE-2016-1185	The Cybozu kintone mobile application 1.x before 1.0.6 for Android allows attackers to discover an authentication token via a crafted application.

Dari Linksys Linux 2.4.X memiliki 47 CVE (hanya sebagian yang ditampilkan)

Search Results

There are **47** CVE entries that match your search.

Name	Description
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-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-2007-4573	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-2007-1357	The atalk_sum_skb function in AppleTalk for Linux kernel 2.6.x before 2.6.21, and possibly 2.4.x, allows remote attackers to cause a denial of service (crash) via an AppleTalk frame that is shorter than the specified length, which triggers a BUG_ON call when an attempt is made to perform a checksum.
CVE-2006-5871	smbfs in Linux kernel 2.6.8 and other versions, and 2.4.x before 2.4.34, when UNIX extensions are enabled, ignores certain mount options, which could cause clients to use server-specified uid, gid and mode settings.
CVE-2006-4093	Linux kernel 2.x.6 before 2.6.17.9 and 2.4.x before 2.4.33.1 on PowerPC PPC970 systems allows local users to cause a denial of service (crash) related to the "HID0 attention enable on PPC970 at boot time."
CVE-2006-3741	The perfmonctl system call (sys_perfmonctl) in Linux kernel 2.4.x and 2.6 before 2.6.18, when running on Itanium systems, does not properly track the reference count for file descriptors, which allows local users to cause a denial of service (file descriptor consumption).
CVE-2006-2071	Linux kernel 2.4.x and 2.6.x up to 2.6.16 allows local users to bypass IPC permissions and modify a readonly attachment of shared memory by using mprotect to give write permission to the attachment. NOTE: some original raw sources combined this issue with CVE-2006-1524, but they are different bugs.
CVE-2006-1242	The ip_push_pending_frames function in Linux 2.4.x and 2.6.x before 2.6.16 increments the IP ID field when sending a RST after receiving unsolicited TCP SYN-ACK packets, which allows remote attackers to conduct an Idle Scan (nmap -sI) attack, which bypasses intended protections against such attacks.
CVE-2006-0096	wan/sdla.c in Linux kernel 2.6.x before 2.6.11 and 2.4.x before 2.4.29 does not require the CAP_SYS_RAWIO privilege for an SDLA firmware upgrade, with unknown impact and local attack vectors. NOTE: further investigation suggests that this issue requires root privileges to exploit, since it is protected by CAP_NET_ADMIN; thus it might not be a

Dari hasil gambar CVE diatas memiliki masing – masing nama dan deskripsi yang berbeda - beda