SCANNING NETWORK
MENGGUNAKAN NMAP DAN CVE

DISUSUN OLEH :

MEILINDA EKA SURYANI (09011181320033)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

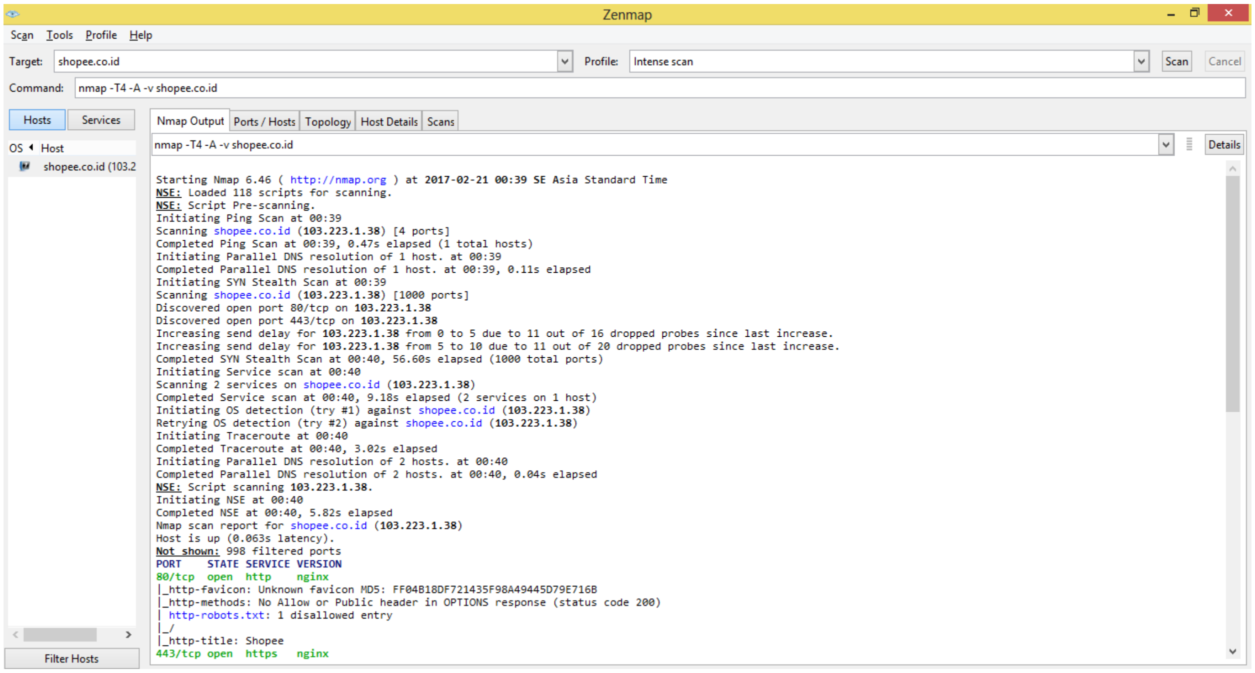
UNIVERSITAS SRIWIJAYA

2016

SCANNING NETWORK MENGGUNAKAN NMAP DAN CVE

Scanning network adalah metode yang digunakan untuk mendapatkan informasi sebanyak-banyaknya dari IP/Network target. Dalam kasus ini target yang discan adalah shopee.co.id. proses *scanning* network ini menggunakan Nmap (*Network Mapping*), yaitu suatu tools 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 apa yang diberikan, sistem operasi apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya.

Langkah awal untuk melakukan *scanning* ialah memasukkan alamat target, dalam hal ini ‘shopee.co.id’, di kolom target yang tersedia pada Nmap/Zenmap, maka pada kolom command akan otomatis menuliskan perintah untuk melakukan *scan*. Pada profile tersedia beberapa pilihan, pilih intense *scan* untuk hasil *scan* yang lebih detail. Lalu klik *scan*, maka didapatkan hasil *scanning*. Dari hasil *scanning*, didapat informasi port yang discan berjumlah 1000 port. Dari 1000 port ini dua diantaranya merupakan open port yaitu port 80/TCP dengan service http versi nginx dan port 443/TCP dengan *service* https versi nginx, sedangkan yang lainnya merupakan *filtered port*. Selain itu Nmap juga menyajikan topologi yang menampilkan hop dari localhost ke target.



Target: shopee.co.id

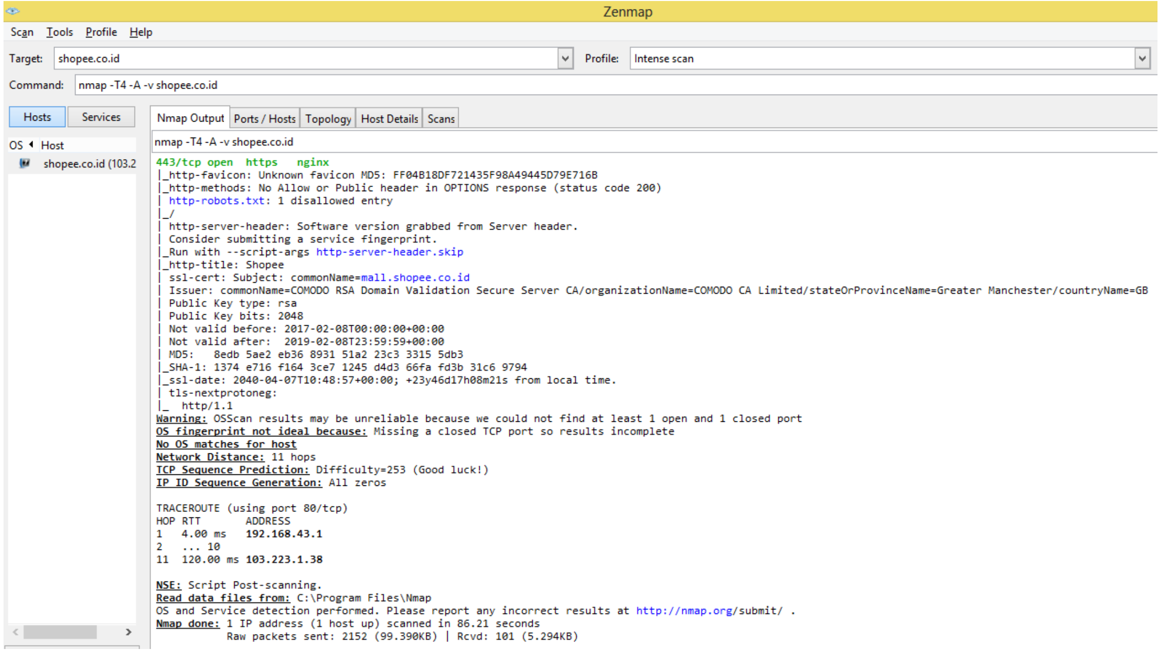
Profile: Intense scan

Command: nmap -T4 -A -v shopee.co.id

nmap -T4 -A -v shopee.co.id

```
Starting Nmap 6.46 ( http://nmap.org ) at 2017-02-21 00:39 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 00:39
Scanning shopee.co.id (103.223.1.38) [4 ports]
Completed Ping Scan at 00:39, 0.47s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:39
Completed Parallel DNS resolution of 1 host. at 00:39, 0.11s elapsed
Initiating SYN Stealth Scan at 00:39
Scanning shopee.co.id (103.223.1.38) [1000 ports]
Discovered open port 80/tcp on 103.223.1.38
Discovered open port 443/tcp on 103.223.1.38
Increasing send delay for 103.223.1.38 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 103.223.1.38 from 5 to 10 due to 11 out of 20 dropped probes since last increase.
Completed SYN Stealth Scan at 00:40, 56.60s elapsed (1000 total ports)
Initiating Service scan at 00:40
Scanning 2 services on shopee.co.id (103.223.1.38)
Completed Service scan at 00:40, 9.18s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against shopee.co.id (103.223.1.38)
Retrying OS detection (try #2) against shopee.co.id (103.223.1.38)
Initiating Traceroute at 00:40
Completed Traceroute at 00:40, 3.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 00:40
Completed Parallel DNS resolution of 2 hosts. at 00:40, 0.04s elapsed
NSE: Script scanning 103.223.1.38.
Initiating NSE at 00:40
Completed NSE at 00:40, 5.82s elapsed
Nmap scan report for shopee.co.id (103.223.1.38)
Host is up (0.063s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    nginx
|_http-favicon: Unknown favicon MD5: FF04B18DF721435F98A49445D79E716B
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Shopee
443/tcp open  https   nginx
```

Gambar 1. Tampilan Nmap Output(1)



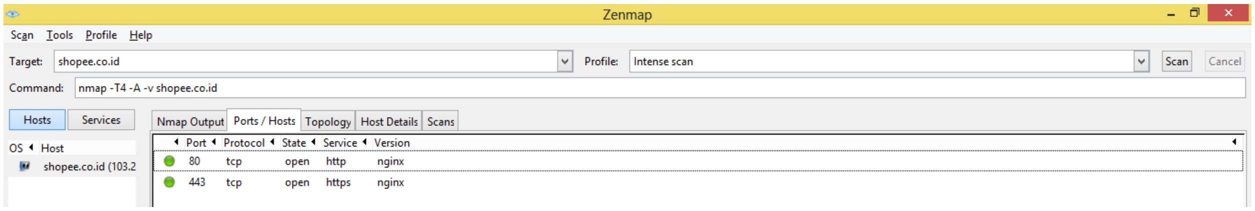
Target: shopee.co.id

Profile: Intense scan

Command: nmap -T4 -A -v shopee.co.id

```
nmap -T4 -A -v shopee.co.id
443/tcp open  https   nginx
|_http-favicon: Unknown favicon MD5: FF04B18DF721435F98A49445D79E716B
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
| http-robots.txt: 1 disallowed entry
|_/
| http-server-header: Software version grabbed from Server header.
| Consider submitting a service fingerprint.
|_Run with --script-args http-server-header.skip
|_http-title: Shopee
| ssl-cert: Subject: commonName=mall.shopee.co.id
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2017-02-08T00:00:00+00:00
| Not valid after:  2019-02-08T23:59:59+00:00
| MD5:   8edb 5ae2 eb36 8931 51a2 23c3 3315 5db3
|_SHA-1: 1374 e716 f164 3ce7 1245 d4d3 66fa fd3b 31c6 9794
|_ssl-date: 2040-04-07T10:48:57+00:00; +23y46d17h08m21s from local time.
| tls-nextprotoneg:
|_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   4.00 ms   192.168.43.1
2   ... 10
11  120.00 ms 103.223.1.38

NSE: Script Post-scanning.
Read data files from: C:\Program Files\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 86.21 seconds
           Raw packets sent: 2152 (99.390KB) | Rcvd: 101 (5.294KB)
```

Gambar 2. Tampilan Nmap Output(2)



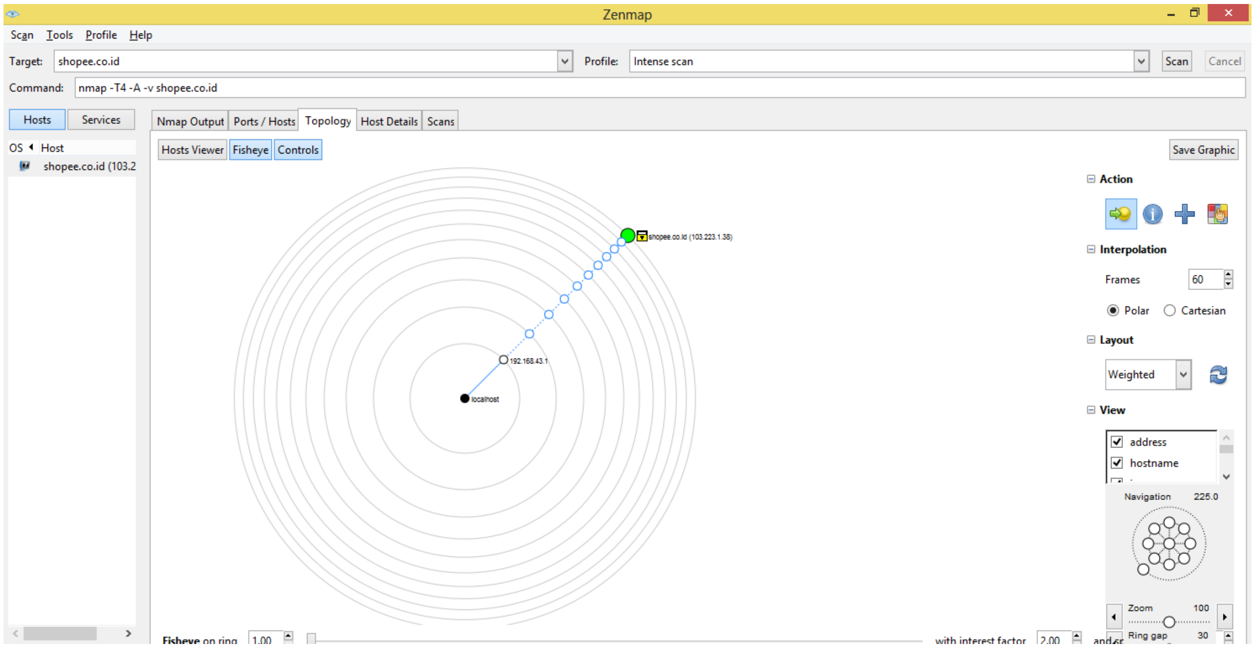
Target: shopee.co.id

Profile: Intense scan

Command: nmap -T4 -A -v shopee.co.id

	Port	Protocol	State	Service	Version
●	80	tcp	open	http	nginx
●	443	tcp	open	https	nginx

Gambar 3. Ports/Hosts pada target

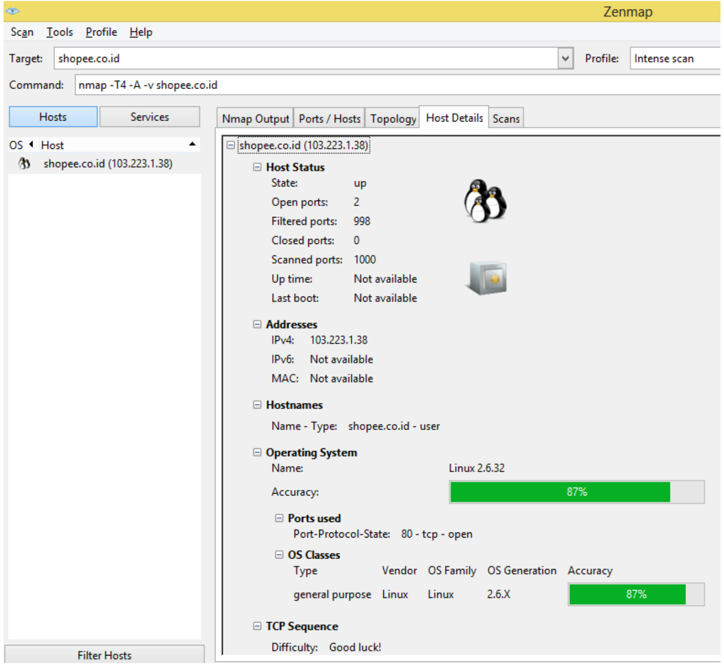


Target: shopee.co.id
Profile: Intense scan
Command: nmap -T4 -A -v shopee.co.id

Frames 60
● Polar ○ Cartesian
Weighted
☑ address
☑ hostname
Navigation 225.0
Zoom 100
Ring gap 30
Fisheye on ring 1.00
with interest factor 2.00

Gambar 4. Topologi hop

Pada *host details*, didapat informasi sistem operasi yang digunakan oleh target. Dalam hal ini target menggunakan sistem operasi Linux 2.6.32. dari informasi ini, kita dapat mencari kelemahan dari sistem operasi yang digunakan target melalui CVE (*Common Vulnerabilities and Exposures*) yang dapat diakses pada http://cve.mitre.org. CVE menyediakan referensi mengenai kelemahan yang ada pada suatu produk, hingga saat ini ada 81977 total CVE ID yang tercatat. Untuk mencari kelemahan Linux 2.6.32 yang diguanakan oleh target ialah dengan cara memasukkan kata kunci ‘Linux 2.6.32’ pada kolom *keyword* yang tersedia, lalu *submit*. Maka akan tampillah hasil pencarian yang berisi nama CVE dan deskripsi kelemahan dari hasil pencarian yang terkait dengan kata kunci. Begitu pula saat mencari kelemahan pada nginx melalui CVE.



Target: shopee.co.id

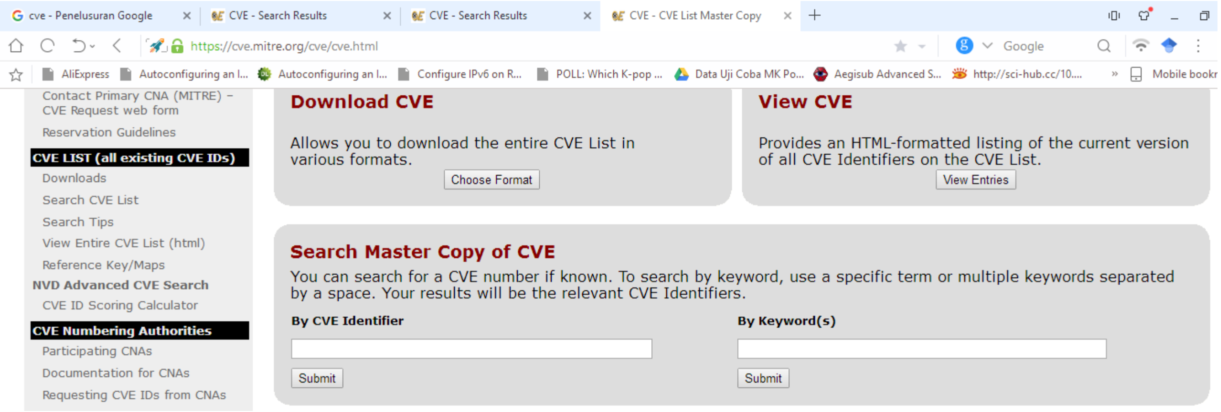
Profile: Intense scan

Command: nmap -T4 -A -v shopee.co.id

shopee.co.id (103.223.1.38)

```
shopee.co.id (103.223.1.38)
  Host Status
    State:            up
    Open ports:       2
    Filtered ports:   998
    Closed ports:     0
    Scanned ports:    1000
    Up time:          Not available
    Last boot:        Not available

  Addresses
    IPv4:   103.223.1.38
    IPv6:   Not available
    MAC:    Not available

  Hostnames
    Name - Type:   shopee.co.id - user

  Operating System
    Name:                      Linux 2.6.32
    Accuracy:                  87%

    Ports used
      Port-Protocol-State:   80 - tcp - open

    OS Classes
      Type              Vendor   OS Family   OS Generation   Accuracy
      general purpose   Linux    Linux       2.6.X           87%

  TCP Sequence
    Difficulty:   Good luck!
```

Gambar 5. Host details



Download CVE

Allows you to download the entire CVE List in various formats.

View CVE

Provides an HTML-formatted listing of the current version of all CVE Identifiers on the CVE List.

Search Master Copy of CVE

You can search for a CVE number if known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Identifiers.

By CVE Identifier

By Keyword(s)

Gambar 6. Tampilan website CVE

Table 1. Hasil pencarian CVE Linux 2.6.32

Name	Description
CVE-2013-2239	vzkernel before 042stab080.2 in the OpenVZ modification for the Linux kernel 2.6.32 does not initialize certain length variables, which allows local users to obtain sensitive information from kernel stack memory via (1) a

	crafted ploop driver ioctl call, related to the ploop_getdevice_ioc function in drivers/block/ploop/dev.c, or (2) a crafted quotactl system call, related to the compat_quotactl function in fs/quota/quota.c.
CVE-2013-2224	A certain Red Hat patch for the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 allows local users to cause a denial of service (invalid free operation and system crash) or possibly gain privileges via a sendmsg system call with the IP_RETOPTS option, as demonstrated by hemlock.c. NOTE: this vulnerability exists because of an incorrect fix for CVE-2012-3552.
CVE-2011-3593	A certain Red Hat patch to the vlan_hwaccel_do_receive function in net/8021q/vlan_core.c in the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 allows remote attackers to cause a denial of service (system crash) via priority-tagged VLAN frames.
CVE-2011-2189	net/core/net_namespace.c in the Linux kernel 2.6.32 and earlier does not properly handle a high rate of creation and cleanup of network namespaces, which makes it easier for remote attackers to cause a denial of service (memory consumption) via requests to a daemon that requires a separate namespace per connection, as demonstrated by vsftpd.
CVE-2011-1576	The Generic Receive Offload (GRO) implementation in the Linux kernel 2.6.18 on Red Hat Enterprise Linux 5 and 2.6.32 on Red Hat Enterprise Linux 6, as used in Red Hat Enterprise Virtualization (RHEV) Hypervisor and other products, allows remote attackers to cause a denial of service via crafted VLAN packets that are processed by the napi_reuse_skb function, leading to (1) a memory leak or (2) memory corruption, a different vulnerability than CVE-2011-1478.
CVE-2011-1020	The proc filesystem implementation in the Linux kernel 2.6.37 and earlier does not restrict access to the /proc directory tree of a process after this process performs an exec of a setuid program, which allows local users to obtain sensitive information or cause a denial of service via open, lseek, read, and write system calls.
CVE-2011-0714	Use-after-free vulnerability in a certain Red Hat patch for the RPC server sockets functionality in the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 might allow remote attackers to cause a denial of service (crash) via malformed data in a packet, related to lockd and the svc_xprt_received function.
CVE-2010-1636	The btrfs_ioctl_clone function in fs/btrfs/ioctl.c in the btrfs functionality in the Linux kernel 2.6.29 through 2.6.32, and possibly other versions, does not ensure that a cloned file descriptor has been opened for reading, which allows local users to read sensitive information from a write-only file descriptor.

CVE-2010-1083	The processcompl_compat function in drivers/usb/core/devio.c in Linux kernel 2.6.x through 2.6.32, and possibly other versions, does not clear the transfer buffer before returning to userspace when a USB command fails, which might make it easier for physically proximate attackers to obtain sensitive information (kernel memory).
CVE-2009-4308	The ext4_decode_error function in fs/ext4/super.c in the ext4 filesystem in the Linux kernel before 2.6.32 allows user-assisted remote attackers to cause a denial of service (NULL pointer dereference), and possibly have unspecified other impact, via a crafted read-only filesystem that lacks a journal.
CVE-2009-4020	Stack-based buffer overflow in the hfs subsystem in the Linux kernel 2.6.32 allows remote attackers to have an unspecified impact via a crafted Hierarchical File System (HFS) filesystem, related to the hfs_readdir function in fs/hfs/dir.c.
CVE-2009-1298	The ip_frag_reasm function in net/ipv4/ip_fragment.c in the Linux kernel 2.6.32-rc8, and 2.6.29 and later versions before 2.6.32, calls IP_INC_STATS_BH with an incorrect argument, which allows remote attackers to cause a denial of service (NULL pointer dereference and hang) via long IP packets, possibly related to the ip_defrag function.

Table 1. Hasil pencarian CVE nginx

Name	Description
CVE-2016-4450	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.
CVE-2016-1247	The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx ebuild before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.
CVE-2016-0747	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause

	a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.
CVE-2016-0746	Use-after-free vulnerability in the resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.
CVE-2016-0742	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.
CVE-2014-3616	nginx 0.5.6 through 1.7.4, when using the same shared ssl_session_cache or ssl_session_ticket_key for multiple servers, can reuse a cached SSL session for an unrelated context, which allows remote attackers with certain privileges to conduct "virtual host confusion" attacks.
CVE-2014-3556	The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.
CVE-2014-0133	Heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request.
CVE-2014-0088	The SPDY implementation in the ngx_http_spdy_module module in nginx 1.5.10 before 1.5.11, when running on a 32-bit platform, allows remote attackers to execute arbitrary code via a crafted request.
CVE-2013-6798	BlackBerry Link before 1.2.1.31 on Windows and before 1.1.1 build 39 on Mac OS X does not properly determine the user account for execution of Peer Manager in certain situations involving successive logins with different accounts, which allows context-dependent attackers to bypass intended restrictions on remote file-access folders via IPv6 WebDAV requests, a different vulnerability than CVE-2013-3694.
CVE-2013-4547	nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.
CVE-2013-3694	BlackBerry Link before 1.2.1.31 on Windows and before 1.1.1 build 39 on Mac OS X does not require authentication for remote file-access folders, which allows remote attackers to read or create arbitrary files via IPv6 WebDAV requests, as demonstrated by a CSRF attack involving DNS rebinding.
CVE-2013-2070	http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers,

	allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.
CVE-2013-2028	The ngx_http_parse_chunked function in http/ngx_http_parse.c in nginx 1.3.9 through 1.4.0 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a chunked Transfer-Encoding request with a large chunk size, which triggers an integer signedness error and a stack-based buffer overflow.
CVE-2013-0337	The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.
CVE-2012-3380	Directory traversal vulnerability in naxsi-ui/nx_extract.py in the Naxsi module before 0.46-1 for Nginx allows local users to read arbitrary files via unspecified vectors.
CVE-2012-2089	Buffer overflow in ngx_http_mp4_module.c in the ngx_http_mp4_module module in nginx 1.0.7 through 1.0.14 and 1.1.3 through 1.1.18, when the mp4 directive is used, allows remote attackers to cause a denial of service (memory overwrite) or possibly execute arbitrary code via a crafted MP4 file.
CVE-2012-1180	Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.
CVE-2011-4963	nginx/Windows 1.3.x before 1.3.1 and 1.2.x before 1.2.1 allows remote attackers to bypass intended access restrictions and access restricted files via (1) a trailing . (dot) or (2) certain "$index_allocation" sequences in a request.
CVE-2011-4315	Heap-based buffer overflow in compression-pointer processing in core/ngx_resolver.c in nginx before 1.0.10 allows remote resolvers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a long response.
CVE-2010-2266	nginx 0.8.36 allows remote attackers to cause a denial of service (crash) via certain encoded directory traversal sequences that trigger memory corruption, as demonstrated using the "%c0.%c0." sequence.
CVE-2010-2263	nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or unparsed content of arbitrary files under the web document root by appending ::$DATA to the URI.
CVE-2009-4611	Mort Bay Jetty 6.x and 7.0.0 writes backtrace data without sanitizing non-printable characters, which might allow remote attackers to modify a

	window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator, related to (1) a string value in the Age parameter to the default URI for the Cookie Dump Servlet in test-jetty-webapp/src/main/java/com/acme/CookieDump.java under cookie/, (2) an alphabetic value in the A parameter to jsp/expr.jsp, or (3) an alphabetic value in the Content-Length HTTP header to an arbitrary application.
CVE-2009-4496	Boa 0.94.14rc21 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4495	Yaws 1.85 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4494	AOLserver 4.5.1 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4493	Orion Application Server 2.0.7 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4492	WEBrick 1.3.1 in Ruby 1.8.6 through patchlevel 383, 1.8.7 through patchlevel 248, 1.8.8dev, 1.9.1 through patchlevel 376, and 1.9.2dev writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4491	thttpd 2.25b0 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4490	mini_httpd 1.19 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4489	header.c in Cherokee before 0.99.32 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to

	modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-4488	** DISPUTED ** Varnish 2.0.6 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator. NOTE: the vendor disputes the significance of this report, stating that "This is not a security problem in Varnish or any other piece of software which writes a logfile. The real problem is the mistaken belief that you can cat(1) a random logfile to your terminal safely."
CVE-2009-4487	nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2009-3898	Directory traversal vulnerability in src/http/modules/ngx_http_dav_module.c in nginx (aka Engine X) before 0.7.63, and 0.8.x before 0.8.17, allows remote authenticated users to create or overwrite arbitrary files via a .. (dot dot) in the Destination HTTP header for the WebDAV (1) COPY or (2) MOVE method.
CVE-2009-3896	src/http/ngx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.14 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a long URI.
CVE-2009-3555	The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.
CVE-2009-2629	Buffer underflow in src/http/ngx_http_parse.c in nginx 0.1.0 through 0.5.37, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.15 allows remote attackers to execute arbitrary code via crafted HTTP requests.