Nama : Riki Andika
NIM : 09011181320015

Hang on Training, Kamis 23 Februari 2017

Network scanner adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network target yang akan dicari titik kelemahannya, kali ini dilakukan scanning dengan menggunakan simulasi yang menggunakan software virtualbox dengan dua sistem operasi linux, dengan 1 OS Linux digunakan sebagai Targen yang akan discan dengan alamat IP yang telah ditentukan 192.168.1.1, dan OS Linux yang satunya dijadikan sebagai penyerang dengan alamat IP 192.168.1.2. Berikut simulasi yang telah dilakukan sebagai berikut;

Code1

```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A4:69:F0
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea4:69f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2706 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:180638 (176.4 KiB)  TX bytes:151660 (148.1 KiB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5152 (5.0 KiB)  TX bytes:5152 (5.0 KiB)

bt ~ #
```

Gambar 1. Ifconfig pada OS Target

Dari gambar diatas dapat dilihat alamat IP yang dimasukkan pada sistem operasi (OS) yang digunakan sebagai target yang akan d scan, dan berikut gambar pengaturan IP Address pada sistem operasi (OS) yang digunakan sebagai penyerang.

Code2

```
root@mahasiswa:/home/mahasiswa# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:be:5d:b9
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.
255.255.0
          inet6 addr: fe80::a00:27ff:febe:5db9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3096 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3266 errors:0 dropped:0 overruns:0 carrier
:0
          collisions:0 txqueuelen:1000
          RX bytes:362190 (362.1 KB)  TX bytes:234084 (234.0 KB
)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:326 errors:0 dropped:0 overruns:0 frame:0
          TX packets:326 errors:0 dropped:0 overruns:0 carrier:
```

Gambar 2. Ifconfig pada OS penyerang

Tahap awal untuk melakukan scan, mengunakan tools yang dapat digunakan untuk scanning suatu website, baik dengan meggunakan tools online ataupun tools yang dipasang (diinstal). Pada percobaan ini menggunakan tools yang diinstal pada sistem dengan tools xprobe2 dan nmap, berikut step-step scanning dengan menggunakan xprobe dan nmap;

Code3

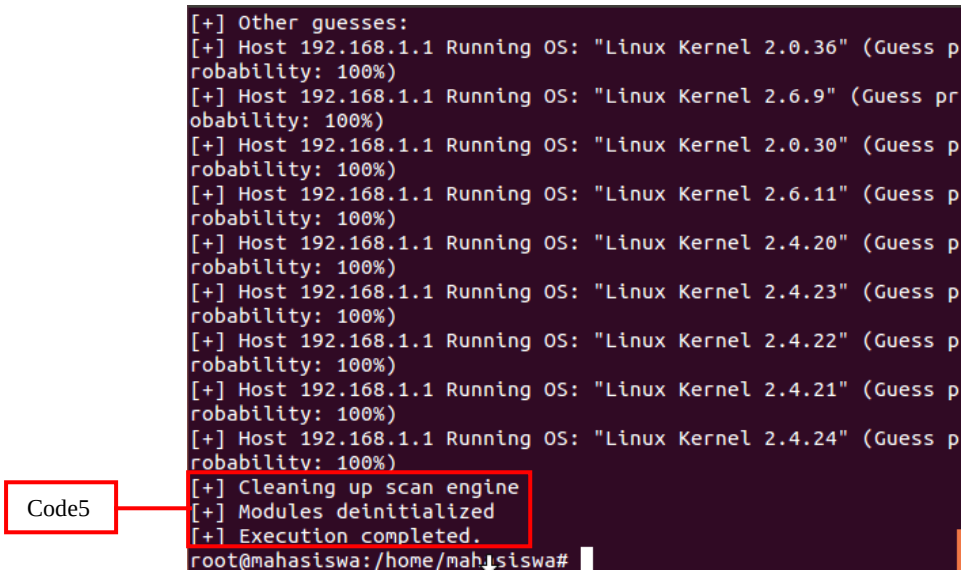
```
root@mahasiswa:/home/mahasiswa# xprobe2 192.168.1.1

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-s
ecurity.com, meder@o0o.nu

[+] Target is 192.168.1.1
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance
calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprint
ing module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fing
erprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fi
ngerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable
 fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprintin
```

Gambar 3.a xprobe2 IP tujuan

Code4

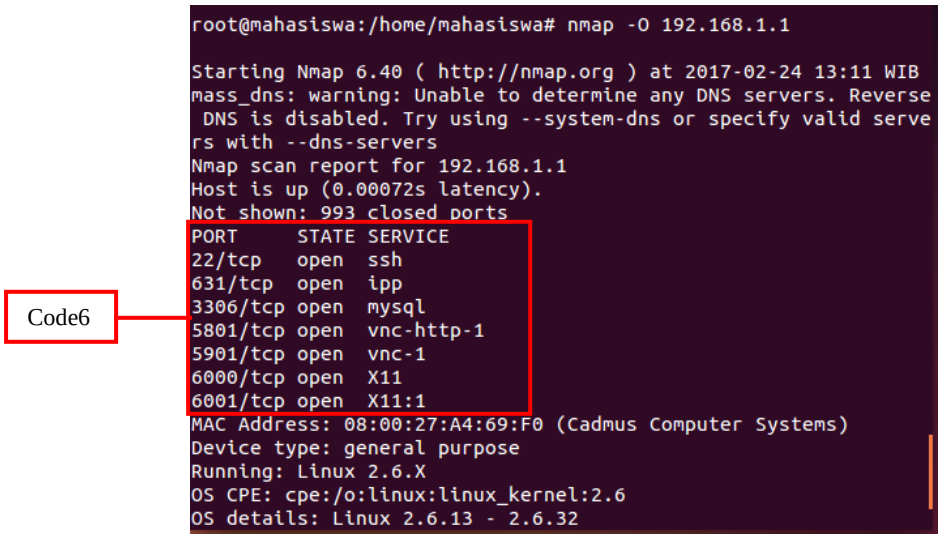
```
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192
.168.1.1. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192
.168.1.1. Module test failed
[-] No distance calculation. 192.168.1.1 appears to be dead or
no ports known
[+] Host: 192.168.1.1 is up (Guess probability: 50%)
[+] Target: 192.168.1.1 is alive. Round-Trip Time: 0.45228 sec
[+] Selected safe Round-Trip Time value is: 0.90455 sec
[-] icmp_port_unreach::build_DNS_reply(): gethostbyname() faile
d! Using static ip for www.securityfocus.com in UDP probe
[-] fingerprint:tcp_hshake Module execution aborted (no open TC
P ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 192.168.1.1 Running OS: "Linux Kernel 2.4.25" (Guess p
robability: 100%)
[+] Other guesses:
```

Gambar 3.b xprobe2 IP tujuan



Gambar 3.c xprobe2 IP tujuan

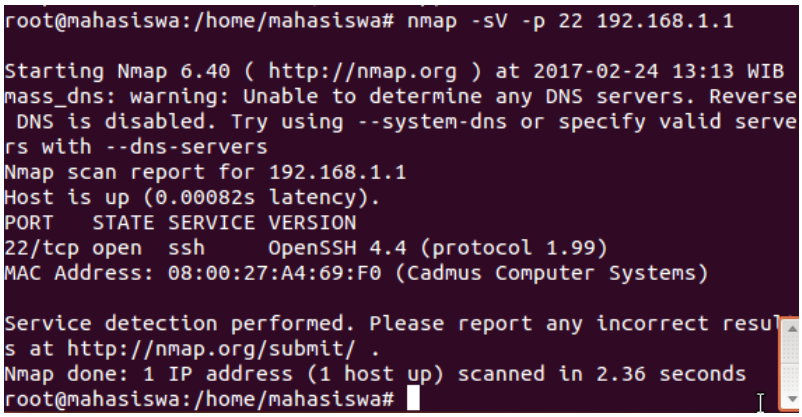
Dari hasil diatas terlihat port yang sedang digunakan dan port yang terbuka dan juga sistem operasi yang digunakan website sasaran, dengan sistem operasi yang digunakan linux kernel versi 2.4.25 (code2). Untuk memastika benar atau tidaknya dapat dicek pada sistem ysng dijadikan sebagai target dengan mengecek sistem operasi yang digunakan, kevalidan data yang digunakan dengan menggunakan perintah *uname –a* pada sistem.



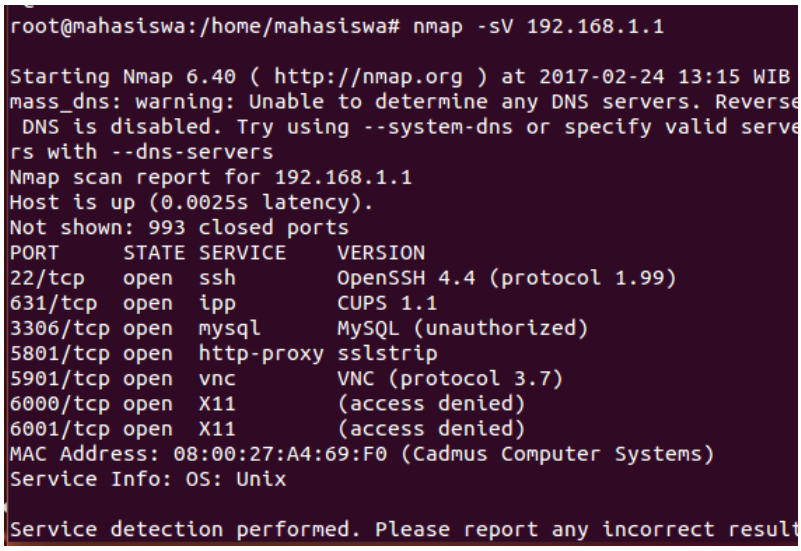
Gambar 4. Nmap –O IP addres

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host,

penyerang harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila penyerang sudah mengetahui bahwa host menjalankan proses SMTP server, maka dapat menggunakan kelemahan-kelemahan yang ada pada SMTP server untuk mendapatkan akses. Dari bagian ini dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi. Pada gambar 4 terdapat 7 PORT yang terbuka aksesnya, hal ini dapat menjadi cela untuk melakukan penyerangan (code6). Perintah nmap –sV IP Tagret merupakan perintah untuk mengetahui host yang sedang aktiv dengan port yang digunakannya, dapat dilihat pada gambar 5.a berikut;



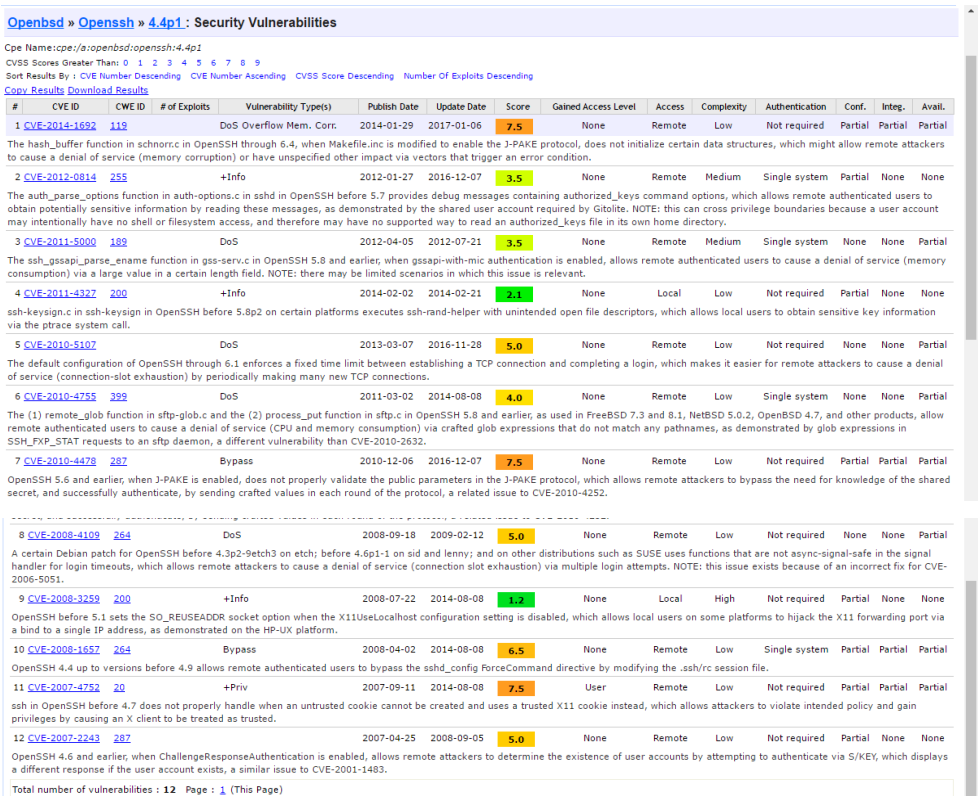
Gambar 5.a nmap –Sv IP Target



Gambar 5.b nmap –Sv IP Target

Pada gambar 5.b dengan perintah yang dijalankan nmap –sV IP Target digunakan unutk melihat PORT mana saja yang terbuka berserta dengan versi sistem yang digunakannya, sehingga sistem dalam keamanannya semakin dapat ditembus, dengan mencari detail kelemahan-kelemahan dari versi sistem yang digunakan. Open Port, Port 22 merupakan port SSH (Secure Shell) merupakan sebuah protokol jaringan yang memanfaatkan kriptografi untuk melakukan komunikasi data pada perangkat jaringan agar lebih aman. Alam konsepnya penggunaan SSH ini harus di dukung oleh server maupun perangkat atau komputer klien yang melakukan pertukaran data. Keduanya harus memiliki SSH server dari sisi komputer server dan SSH klien untuk komputer penerima (klien). Berikut CVE mapping dari gambar 5.b;

a. PORT 22/TCP



Openbsd » Openssh » 4.4p1 : Security Vulnerabilities

Cpe Name:*cpe:/a:openbsd:openssh:4.4p1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

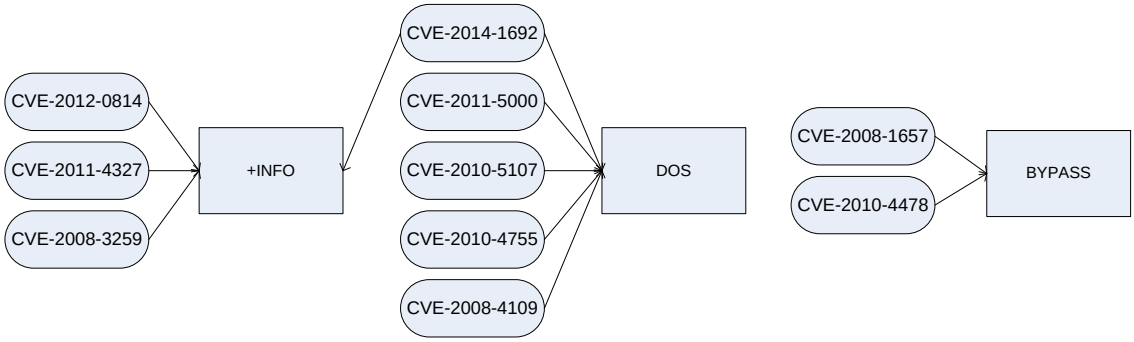
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-1692	119		DoS Overflow Mem. Corr.	2014-01-29	2017-01-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.														
2	CVE-2012-0814	255		+Info	2012-01-27	2016-12-07	3.5	None	Remote	Medium	Single system	Partial	None	None
The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.														
3	CVE-2011-5000	189		DoS	2012-04-05	2012-07-21	3.5	None	Remote	Medium	Single system	None	None	Partial
The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.														
4	CVE-2011-4327	200		+Info	2014-02-02	2014-02-21	2.1	None	Local	Low	Not required	Partial	None	None
ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.														
5	CVE-2010-5107			DoS	2013-03-07	2016-11-28	5.0	None	Remote	Low	Not required	None	None	Partial
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.														
6	CVE-2010-4755	399		DoS	2011-03-02	2014-08-08	4.0	None	Remote	Low	Single system	None	None	Partial
The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.														
7	CVE-2010-4478	287		Bypass	2010-12-06	2016-12-07	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.														
8	CVE-2008-4109	264		DoS	2008-09-18	2009-02-12	5.0	None	Remote	Low	Not required	None	None	Partial
A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch; before 4.6p1-1 on sid and lenny; and on other distributions such as SUSE uses functions that are not async-signal-safe in the signal handler for login timeouts, which allows remote attackers to cause a denial of service (connection slot exhaustion) via multiple login attempts. NOTE: this issue exists because of an incorrect fix for CVE-2006-5051.														
9	CVE-2008-3259	200		+Info	2008-07-22	2014-08-08	1.2	None	Local	High	Not required	Partial	None	None
OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.														
10	CVE-2008-1657	264		Bypass	2008-04-02	2014-08-08	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
OpenSSH 4.4 up to versions before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the .ssh/rc session file.														
11	CVE-2007-4752	20		+Priv	2007-09-11	2014-08-08	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.														
12	CVE-2007-2243	287			2007-04-25	2008-09-05	5.0	None	Remote	Low	Not required	Partial	None	None
OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.														

Total number of vulnerabilities : 12 Page : 1 (This Page)

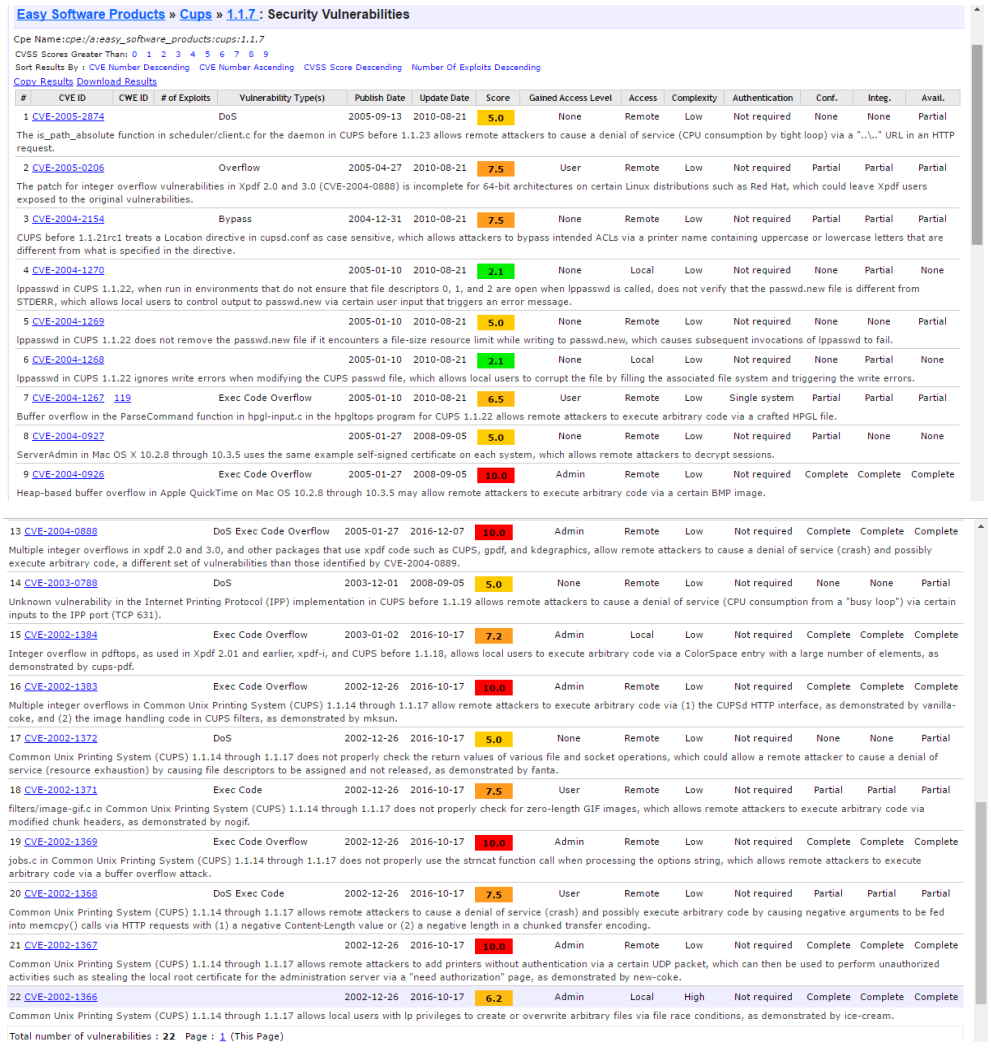
Gambar 6. Hasil CVE Open SSH 4.4

Dari Hasil CVE diatas dibuat suatu diagram yang yang menunjukkan Vulnerability dari penggunaan SSH yang ada, berikut diagramnya;



Gambar 7. Mapping CVE Open SSH 4.4

b. PORT 631/TCP IPP versi CUPS 1.1



Easy Software Products » Cups » 1.1.7 : Security Vulnerabilities

Cpe Name:*cpe:/a:easy_software_products:cups:1.1.7*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

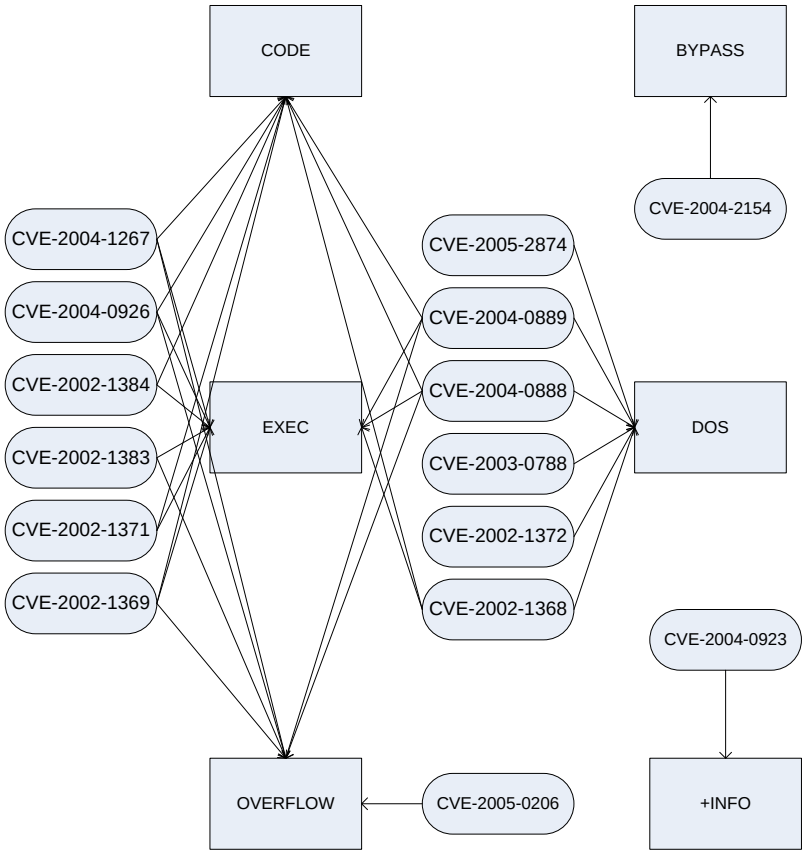
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2005-2874			DoS	2005-09-13	2010-08-21	5.0	None	Remote	Low	Not required	None	None	Partial
The is_path_absolute function in scheduler/client.c for the daemon in CUPS before 1.1.23 allows remote attackers to cause a denial of service (CPU consumption by tight loop) via a "..\.." URL in an HTTP request.														
2	CVE-2005-0206			Overflow	2005-04-27	2010-08-21	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
The patch for integer overflow vulnerabilities in Xpdf 2.0 and 3.0 (CVE-2004-0888) is incomplete for 64-bit architectures on certain Linux distributions such as Red Hat, which could leave Xpdf users exposed to the original vulnerabilities.														
3	CVE-2004-2154			Bypass	2004-12-31	2010-08-21	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
CUPS before 1.1.21rc1 treats a Location directive in cupsd.conf as case sensitive, which allows attackers to bypass intended ACLs via a printer name containing uppercase or lowercase letters that are different from what is specified in the directive.														
4	CVE-2004-1270				2005-01-10	2010-08-21	2.1	None	Local	Low	Not required	None	Partial	None
lppasswd in CUPS 1.1.22, when run in environments that do not ensure that file descriptors 0, 1, and 2 are open when lppasswd is called, does not verify that the passwd.new file is different from STDERR, which allows local users to control output to passwd.new via certain user input that triggers an error message.														
5	CVE-2004-1269				2005-01-10	2010-08-21	5.0	None	Remote	Low	Not required	None	None	Partial
lppasswd in CUPS 1.1.22 does not remove the passwd.new file if it encounters a file-size resource limit while writing to passwd.new, which causes subsequent invocations of lppasswd to fail.														
6	CVE-2004-1268				2005-01-10	2010-08-21	2.1	None	Local	Low	Not required	None	Partial	None
lppasswd in CUPS 1.1.22 ignores write errors when modifying the CUPS passwd file, which allows local users to corrupt the file by filling the associated file system and triggering the write errors.														
7	CVE-2004-1267	119		Exec Code Overflow	2005-01-10	2010-08-21	6.5	User	Remote	Low	Single system	Partial	Partial	Partial
Buffer overflow in the ParseCommand function in hpgl-input.c in the hpgltops program for CUPS 1.1.22 allows remote attackers to execute arbitrary code via a crafted HPGL file.														
8	CVE-2004-0927				2005-01-27	2008-09-05	5.0	None	Remote	Low	Not required	Partial	None	None
ServerAdmin in Mac OS X 10.2.8 through 10.3.5 uses the same example self-signed certificate on each system, which allows remote attackers to decrypt sessions.														
9	CVE-2004-0926			Exec Code Overflow	2005-01-27	2008-09-05	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Heap-based buffer overflow in Apple QuickTime on Mac OS 10.2.8 through 10.3.5 may allow remote attackers to execute arbitrary code via a certain BMP image.														
13	CVE-2004-0888			DoS Exec Code Overflow	2005-01-27	2016-12-07	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Multiple integer overflows in xpdf 2.0 and 3.0, and other packages that use xpdf code such as CUPS, gpdf, and kdegraphics, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code, a different set of vulnerabilities than those identified by CVE-2004-0889.														
14	CVE-2003-0788			DoS	2003-12-01	2008-09-05	5.0	None	Remote	Low	Not required	None	None	Partial
Unknown vulnerability in the Internet Printing Protocol (IPP) implementation in CUPS before 1.1.19 allows remote attackers to cause a denial of service (CPU consumption from a "busy loop") via certain inputs to the IPP port (TCP 631).														
15	CVE-2002-1384			Exec Code Overflow	2003-01-02	2016-10-17	7.2	Admin	Local	Low	Not required	Complete	Complete	Complete
Integer overflow in pdftops, as used in Xpdf 2.01 and earlier, xpdf-i, and CUPS before 1.1.18, allows local users to execute arbitrary code via a ColorSpace entry with a large number of elements, as demonstrated by cups-pdf.														
16	CVE-2002-1383			Exec Code Overflow	2002-12-26	2016-10-17	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Multiple integer overflows in Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allow remote attackers to execute arbitrary code via (1) the CUPSd HTTP interface, as demonstrated by vanilla-coke, and (2) the image handling code in CUPS filters, as demonstrated by mksun.														
17	CVE-2002-1372			DoS	2002-12-26	2016-10-17	5.0	None	Remote	Low	Not required	None	None	Partial
Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 does not properly check the return values of various file and socket operations, which could allow a remote attacker to cause a denial of service (resource exhaustion) by causing file descriptors to be assigned and not released, as demonstrated by fanta.														
18	CVE-2002-1371			Exec Code	2002-12-26	2016-10-17	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
filters/image-gif.c in Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 does not properly check for zero-length GIF images, which allows remote attackers to execute arbitrary code via modified chunk headers, as demonstrated by nogif.														
19	CVE-2002-1369			Exec Code Overflow	2002-12-26	2016-10-17	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
jobs.c in Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 does not properly use the strncat function call when processing the options string, which allows remote attackers to execute arbitrary code via a buffer overflow attack.														
20	CVE-2002-1368			DoS Exec Code	2002-12-26	2016-10-17	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by causing negative arguments to be fed into memcpy() calls via HTTP requests with (1) a negative Content-Length value or (2) a negative length in a chunked transfer encoding.														
21	CVE-2002-1367				2002-12-26	2016-10-17	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows remote attackers to add printers without authentication via a certain UDP packet, which can then be used to perform unauthorized activities such as stealing the local root certificate for the administration server via a "need authorization" page, as demonstrated by new-coke.														
22	CVE-2002-1366				2002-12-26	2016-10-17	6.2	Admin	Local	High	Not required	Complete	Complete	Complete
Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows local users with lp privileges to create or overwrite arbitrary files via file race conditions, as demonstrated by ice-cream.														

Total number of vulnerabilities : 22 Page : 1 (This Page)

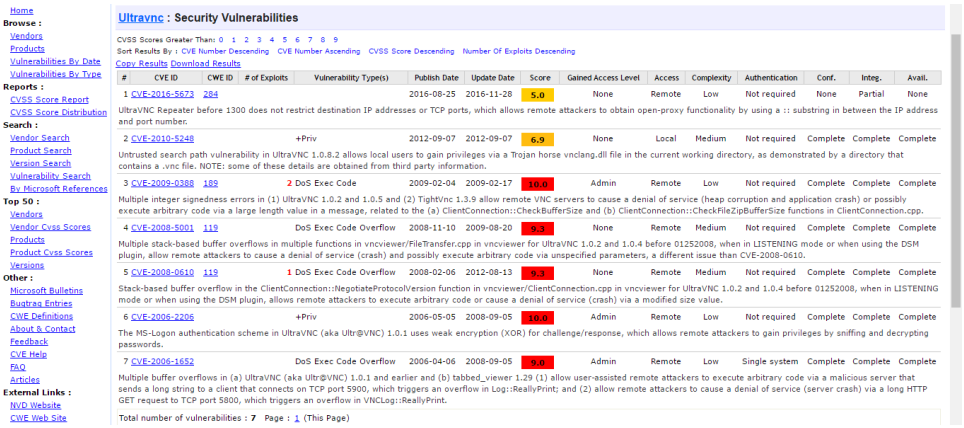
Gambar 8. Hasil CVE IPP versi CUPS 1.1

Dari Hasil CVE diatas dibuat suatu diagram yang yang menunjukkan Vulnerability dari penggunaan SSH yang ada, berikut diagramnya;



Gambar 9. Mapping CVE IPP versi CUPS 1.1

c. PORT 5901/TCP VNC (PROTOCOL 3.7)



Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site

Ultravnc : Security Vulnerabilities

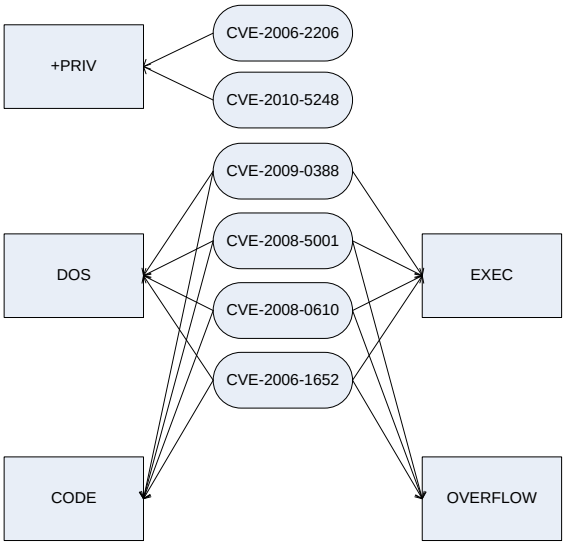
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-5673	284			2016-08-25	2016-11-28	5.0	None	Remote	Low	Not required	None	Partial	None
	UltraVNC Repeater before 1300 does not restrict destination IP addresses or TCP ports, which allows remote attackers to obtain open-proxy functionality by using a :: substring in between the IP address and port number.													
2	CVE-2010-5248			+Priv	2012-09-07	2012-09-07	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
	Untrusted search path vulnerability in UltraVNC 1.0.8.2 allows local users to gain privileges via a Trojan horse vnclang.dll file in the current working directory, as demonstrated by a directory that contains a .vnc file. NOTE: some of these details are obtained from third party information.													
3	CVE-2009-0388	189	2	DoS Exec Code	2009-02-04	2009-02-17	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	Multiple integer signedness errors in (1) UltraVNC 1.0.2 and 1.0.5 and (2) TightVnc 1.3.9 allow remote VNC servers to cause a denial of service (heap corruption and application crash) or possibly execute arbitrary code via a large length value in a message, related to the (a) ClientConnection::CheckBufferSize and (b) ClientConnection::CheckFileZipBufferSize functions in ClientConnection.cpp.													
4	CVE-2008-5001	119		DoS Exec Code Overflow	2008-11-10	2009-08-20	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	Multiple stack-based buffer overflows in multiple functions in vncviewer/FileTransfer.cpp in vncviewer for UltraVNC 1.0.2 and 1.0.4 before 01252008, when in LISTENING mode or when using the DSM plugin, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified parameters, a different issue than CVE-2008-0610.													
5	CVE-2008-0610	119	1	DoS Exec Code Overflow	2008-02-06	2012-08-13	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	Stack-based buffer overflow in the ClientConnection::NegotiateProtocolVersion function in vncviewer/ClientConnection.cpp in vncviewer for UltraVNC 1.0.2 and 1.0.4 before 01252008, when in LISTENING mode or when using the DSM plugin, allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a modified size value.													
6	CVE-2006-2206			+Priv	2006-05-05	2008-09-05	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
	The MS-Logon authentication scheme in UltraVNC (aka Ultr@VNC) 1.0.1 uses weak encryption (XOR) for challenge/response, which allows remote attackers to gain privileges by sniffing and decrypting passwords.													
7	CVE-2006-1652			DoS Exec Code Overflow	2006-04-06	2008-09-05	9.0	Admin	Remote	Low	Single system	Complete	Complete	Complete
	Multiple buffer overflows in (a) UltraVNC (aka Ultr@VNC) 1.0.1 and earlier and (b) tabbed_viewer 1.29 (1) allow user-assisted remote attackers to execute arbitrary code via a malicious server that sends a long string to a client that connects on TCP port 5900, which triggers an overflow in Log::ReallyPrint; and (2) allow remote attackers to cause a denial of service (server crash) via a long HTTP GET request to TCP port 5800, which triggers an overflow in VNCLog::ReallyPrint.													

Total number of vulnerabilities : 7 Page : 1 (This Page)

Gambar 10. CVE VNC (PROTOCOL 3.7)

Dari Hasil CVE diatas dibuat suatu diagram yang yang menunjukkan Vulnerability dari penggunaan SSH yang ada, berikut diagramnya;



Gambar 11. Mapping VNC (PROTOCOL 3.7)

Pada tugas 2 sebelumnya, dengan website target www.polsri.ac.id dengan alamat IP 202.9.69.34, berikut hasil CVE yang dihasilkan beserta Mapping dari CV yang dihasilkan, dengan menggunakan tools nmap dilakukan scan dengan tujuan IP address target, berikut hasil scan yang diperoleh dengan dua PORT yang terbuka;

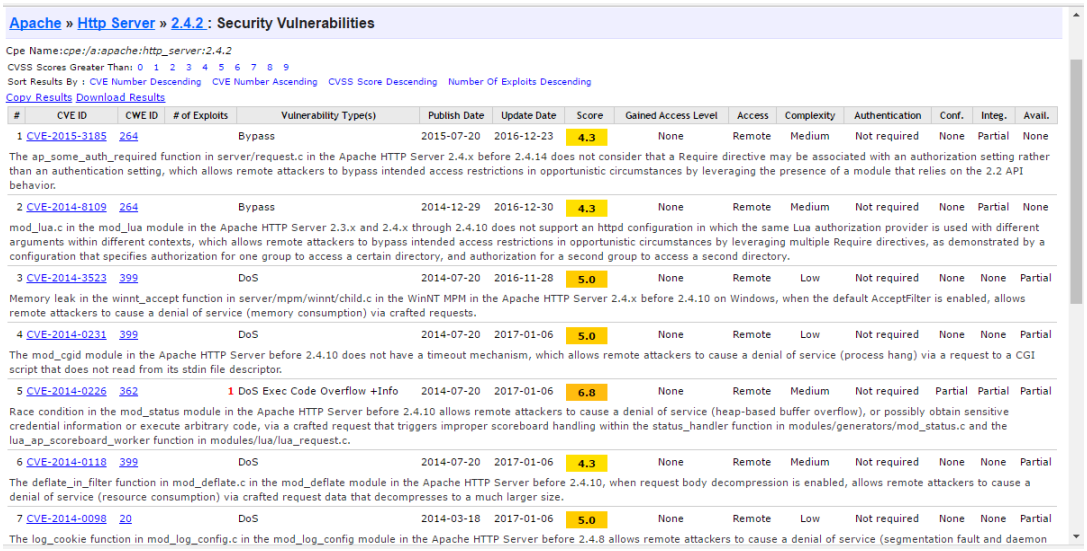
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Riki>ping polsri.ac.id

Pinging polsri.ac.id [202.9.69.34] with 32 bytes of data:
Reply from 202.9.69.34: bytes=32 time=42ms TTL=56
Reply from 202.9.69.34: bytes=32 time=42ms TTL=56
Reply from 202.9.69.34: bytes=32 time=44ms TTL=56
Reply from 202.9.69.34: bytes=32 time=42ms TTL=56

Ping statistics for 202.9.69.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 42ms

C:\Users\Riki>nmap -sV 202.9.69.34

Starting Nmap 6.46 ( http://nmap.org ) at 2017-02-25 14:35 SE Asia Standard Tim

Nmap scan report for www.polsri.ac.id (202.9.69.34)
Host is up (0.044s latency).
Not shown: 972 closed ports, 26 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache
8254/tcp open  http-proxy Squid http proxy 2.6.STABLE21

Service detection performed. Please report any incorrect results at http://nmap
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.72 seconds

C:\Users\Riki>
```

Code7

Gambar 12. Hasil scan dengan tools nmap

a. PORT 80/TCP Apace

Hasil screenshoot dari pencarian CVE dan Mappingnya



Apache » Http Server » 2.4.2 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.4.2*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

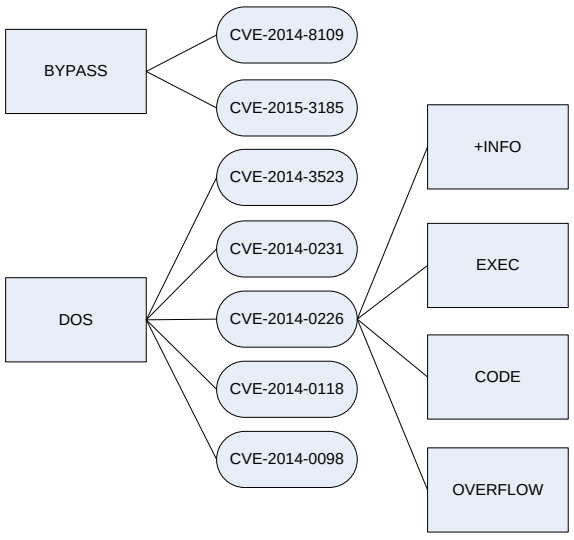
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2015-3185	264		Bypass	2015-07-20	2016-12-23	4.3	None	Remote	Medium	Not required	None	Partial	None
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.														
2	CVE-2014-8109	264		Bypass	2014-12-29	2016-12-30	4.3	None	Remote	Medium	Not required	None	Partial	None
mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.														
3	CVE-2014-3523	399		DoS	2014-07-20	2016-11-28	5.0	None	Remote	Low	Not required	None	None	Partial
Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.														
4	CVE-2014-0231	399		DoS	2014-07-20	2017-01-06	5.0	None	Remote	Low	Not required	None	None	Partial
The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.														
5	CVE-2014-0226	362	1	DoS Exec Code Overflow +Info	2014-07-20	2017-01-06	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.														
6	CVE-2014-0118	399		DoS	2014-07-20	2017-01-06	4.3	None	Remote	Medium	Not required	None	None	Partial
The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.														
7	CVE-2014-0098	20		DoS	2014-03-18	2017-01-06	5.0	None	Remote	Low	Not required	None	None	Partial
The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon														

Gambar 13. CVE PORT 80/CVE Apace

Dari Hasil CVE diatas dibuat suatu diagram yang yang menunjukkan Vulnerability dari penggunaan SSH yang ada, berikut diagramnya;



b. PORT 8254/TCP Squid http proxy 2.6 Stable21

Squid : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

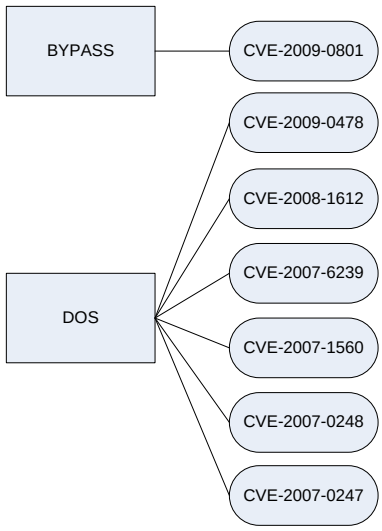
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2009-0801	264		Bypass	2009-03-04	2009-06-18	5.4	None	Remote	High	Not required	Complete	None	None
	Squid, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.													
2	CVE-2009-0478	20	1	DoS	2009-02-08	2009-08-18	5.0	None	Remote	Low	Not required	None	None	Partial
	Squid 2.7 to 2.7.STABLE5, 3.0 to 3.0.STABLE12, and 3.1 to 3.1.0.4 allows remote attackers to cause a denial of service via an HTTP request with an invalid version number, which triggers a reachable assertion in (1) HttpMsg.c and (2) HttpStatusLine.c.													
3	CVE-2008-1612	20		DoS	2008-04-01	2013-07-27	4.3	None	Remote	Medium	Not required	None	None	Partial
	The arrayShrink function (lib/Array.c) in Squid 2.6.STABLE17 allows attackers to cause a denial of service (process exit) via unknown vectors that cause an array to shrink to 0 entries, which triggers an assert error. NOTE: this issue is due to an incorrect fix for CVE-2007-6239.													
4	CVE-2007-6239	20		DoS	2007-12-04	2010-08-21	5.0	None	Remote	Low	Not required	None	None	Partial
	The "cache update reply processing" functionality in Squid 2.x before 2.6.STABLE17 and Squid 3.0 allows remote attackers to cause a denial of service (crash) via unknown vectors related to HTTP headers and an Array memory leak during requests for cached objects.													
5	CVE-2007-1560			DoS	2007-03-21	2011-07-13	5.0	None	Remote	Low	Not required	None	None	Partial
	The clientProcessRequest() function in src/client_side.c in Squid 2.6 before 2.6.STABLE12 allows remote attackers to cause a denial of service (daemon crash) via crafted TRACE requests that trigger an assertion error.													
6	CVE-2007-0248			DoS	2007-01-16	2010-09-15	5.0	None	Remote	Low	Not required	None	None	Partial
	The aclMatchExternal function in Squid before 2.6.STABLE7 allows remote attackers to cause a denial of service (crash) by causing an external_acl queue overload, which triggers an infinite loop.													
7	CVE-2007-0247	399		DoS	2007-01-16	2010-09-15	5.0	None	Remote	Low	Not required	None	None	Partial
	squid/src/ftp.c in Squid before 2.6.STABLE7 allows remote FTP servers to cause a denial of service (core dump) via crafted FTP directory listing responses, possibly related to the (1) ftpListingFinish and (2) ftpHtmlifyListEntry functions.													
8	CVE-2005-3322			DoS	2005-10-27	2008-09-10	5.0	None	Remote	Low	Not required	None	None	Partial
	Unspecified vulnerability in Squid on SUSE Linux 9.0 allows remote attackers to cause a denial of service (crash) via HTTPs (SSL).													
9	CVE-2005-3258			DoS	2005-10-20	2008-09-05	5.0	None	Remote	Low	Not required	None	None	Partial
	The rfc1738_do_escape function in ftp.c for Squid 2.5 STABLE11 and earlier allows remote FTP servers to cause a denial of service (segmentation fault) via certain "odd" responses.													

Gambar 15. CVE Squid http proxy 2.6 Stable21

Dari Hasil CVE diatas dibuat suatu diagram yang yang menunjukkan Vulnerability dari penggunaan SSH yang ada, berikut diagramnya;



Gambar 16. Mapping CVE Squid http proxy 2.6 Stable21