系統與網路安全實驗 lab1
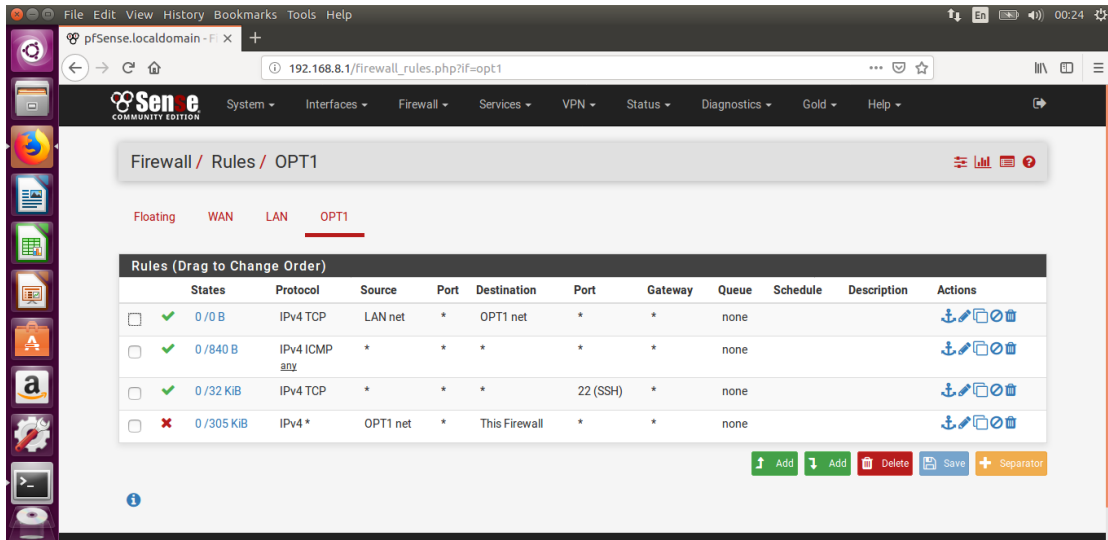
B04902103 資工四 蔡昀達

1. Please write your rules, and write down why should you set up those rules.

1 Allow admin to nmap scan A, B

2 Allow everyone to ping each other

3 Allow A, B to ssh admin

4 Block to access firewall unless in whitelist
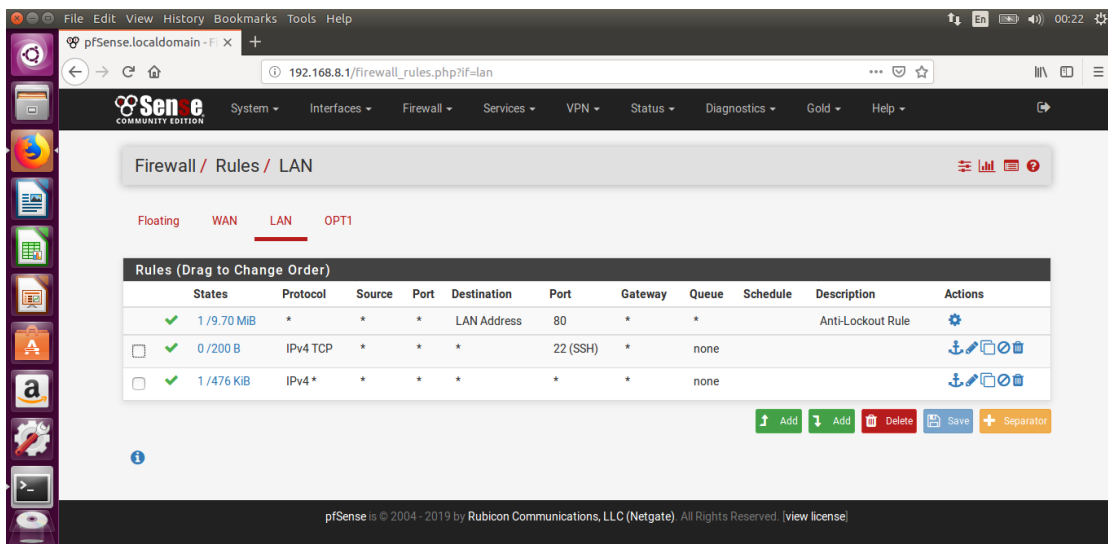
Allow admin to access firewall, ping and ssh.

2. Please write down 3 cpe(OS, Application, hardware)

- cpe:/a:google:chrome:2.0.172
- cpe:/o:linux:kernel:2.6.11.4
- cpe:/h:mcafee:web_gateway:7.0

3. Please write down corresponding CVE for your cpe.

- cpe:/a:google:chrome:2.0.172

Google » Chrome » 2.0.172 : Security Vulnerabilities Published In 2009

Cpe Name:*cpe:/a:google:chrome:2.0.172*
2009 : January February March April May June July August September October November December 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-2009-3934			DoS	2009-11-12	2017-08-16	4.3	None	Remote	Medium	Not required	None	None	Partial

The WebFrameLoaderClient::dispatchDidChangeLocationWithinPage function in src/webkit/glue/webframeloaderclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.

2	CVE-2009-3932			DoS Exec Code Mem. Corr.	2009-11-12	2009-11-13	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

The Gears plugin in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service (memory corruption and plugin crash) or possibly execute arbitrary code via unspecified use of the Gears SQL API, related to putting "SQL metadata into a bad state."

3	CVE-2009-3931	20			2009-11-12	2017-08-16	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete

Incomplete blacklist vulnerability in browser/download/download_exe.cc in Google Chrome before 3.0.195.32 allows remote attackers to force the download of certain dangerous files via a "Content-Disposition: attachment" designation, as demonstrated by (1) .mht and (2) .mhtml files, which are automatically executed by Internet Explorer 6; (3) .svg files, which are automatically executed by Safari; (4) .xml files; (5) .htt files; (6) .xsl files; (7) .xslt files; and (8) image files that are forbidden by the victim's site policy.

4	CVE-2009-3456	310			2009-09-29	2009-09-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

Google Chrome, possibly 3.0.195.21 and earlier, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows

- cpe:/o:linux:kernel:2.6.11.4

Linux » Linux Kernel » 2.6.11.4 : Security Vulnerabilities

Cpe Name:*cpe:/o:linux:linux_kernel:2.6.11.4*
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
Total number of vulnerabilities : 496 Page : 1 (This Page)2 3 4 5 6 7 8 9 10
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-2019-11190	362		Bypass	2019-04-11	2019-04-15	4.7	None	Local	Medium	Not required	Complete	None	None

The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_creds() is called too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat.

2	CVE-2019-10124	94		DoS	2019-03-27	2019-04-11	7.8	None	Remote	Low	Not required	None	None	Complete

An issue was discovered in the hwpoison implementation in mm/memory-failure.c in the Linux kernel before 5.0.4. When soft_offline_in_use_page() runs on a thp tail page after pmd is split, an attacker can cause a denial of service (BUG).

3	CVE-2019-9003	416		Exec Code	2019-02-22	2019-04-02	7.8	None	Remote	Low	Not required	None	None	Complete

In the Linux kernel before 4.20.5, attackers can trigger a drivers/char/ipmi/ipmi_msghandler.c use-after-free and OOPS by arranging for certain simultaneous execution of the code, as demonstrated by a "service ipmievd restart" loop.

4	CVE-2019-8956	416			2019-04-01	2019-04-03	7.2	None	Local	Low	Not required	Complete	Complete	Complete

In the Linux Kernel before versions 4.20.8 and 4.19.21 a use-after-free error in the "sctp_sendmsg()" function (net/sctp/socket.c) when handling SCTP_SENDALL flag can be exploited to corrupt memory.

5	CVE-2019-7308	189			2019-02-01	2019-04-18	4.7	None	Local	Medium	Not required	Complete	None	None

kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on pointer arithmetic in various cases, including cases of different branches with

- cpe:/h:mcafee:web_gateway:7.0

Mcafee » Web Gateway » 7.4.0 : Security Vulnerabilities

Cpe Name:*cpe:/a:mcafee:web_gateway:7.4.0*
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-2014-2535	22		Dir. Trav.	2014-03-18	2018-12-13	4.0	None	Remote	Low	Single system	Partial	None	None

Directory traversal vulnerability in McAfee Web Gateway (MWG) 7.4.x before 7.4.1, 7.3.x before 7.3.2.6, and 7.2.0.9 and earlier allows remote authenticated users to read arbitrary files via a crafted request to the web filtering port.

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