测试标题

someone@somecorp.com

[OUTLINE]

- 漏洞与利用
- 分工专业化
- 黑客

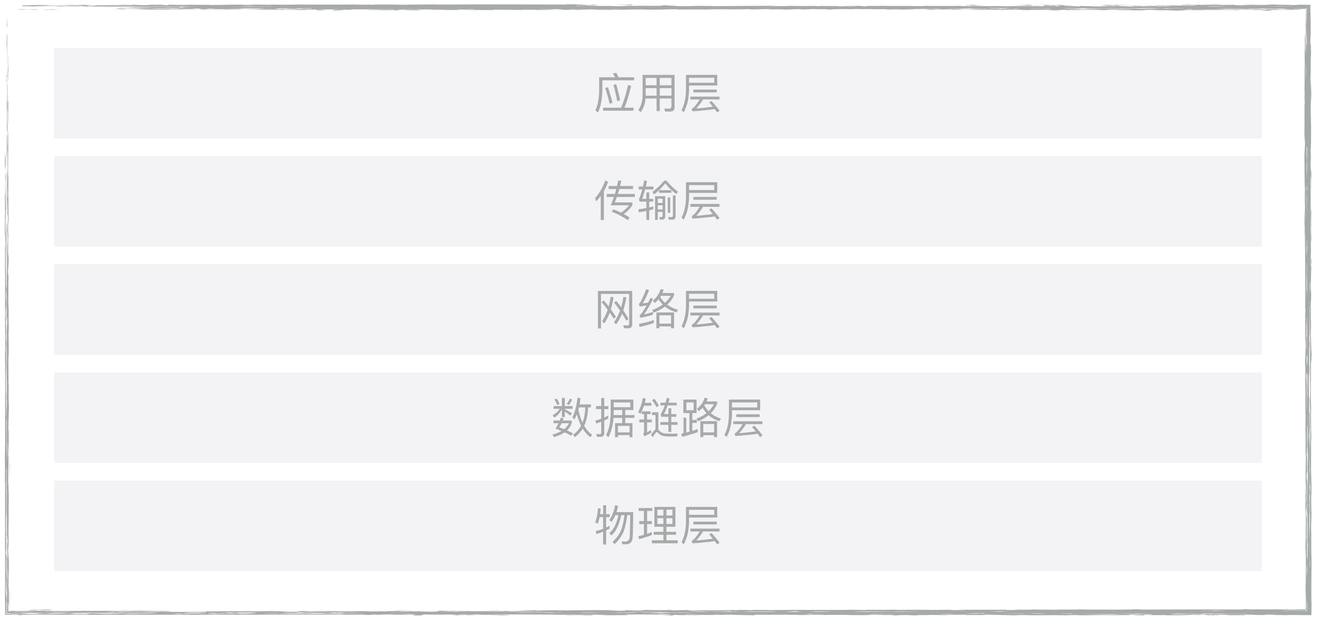
漏洞的表现形式

- 程序逻辑可被控制/改变
  - 代码选择执行
  - 可注入代码
- 程序逻辑可被滥用

攻击某个程序的一个前提是需要与相关代码进行数据交互的渠道：

- 可以与目标进行各种本地进程间的通信
- 可以与目标程序进行网络间进程通信

利用协议栈



利用协议栈

```
[root@cloud ~]# nmap 67.229.128.67 --scanflags SYN,FIN -p 3399

Starting Nmap 5.51 ( http://nmap.org ) at 2014-06-03 17:44 CST
Nmap scan report for 67.229.128.67
Host is up (0.16s latency).
PORT     STATE SERVICE
3399/tcp open  sapeps

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
[root@cloud ~]#
```

```
[root@cloud ~]# tcpdump -i seth0 host 67.229.128.67 and port 3399 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol dec
ode
listening on seth0, link-type EN10MB (Ethernet), capture size 65535 byt
es
17:44:43.849769 IP 101.78.230.76.62034 > 67.229.128.67.3399: Flags [FS]
, seq 3794892674, win 4096, options [mss 1460], length 0
17:44:44.038355 IP 67.229.128.67.3399 > 101.78.230.76.62034: Flags [S.]
, seq 2179667586, ack 3794892675, win 16384, options [mss 1460], length
 0
17:44:44.038386 IP 101.78.230.76.62034 > 67.229.128.67.3399: Flags [R],
 seq 3794892675, win 0, length 0
```

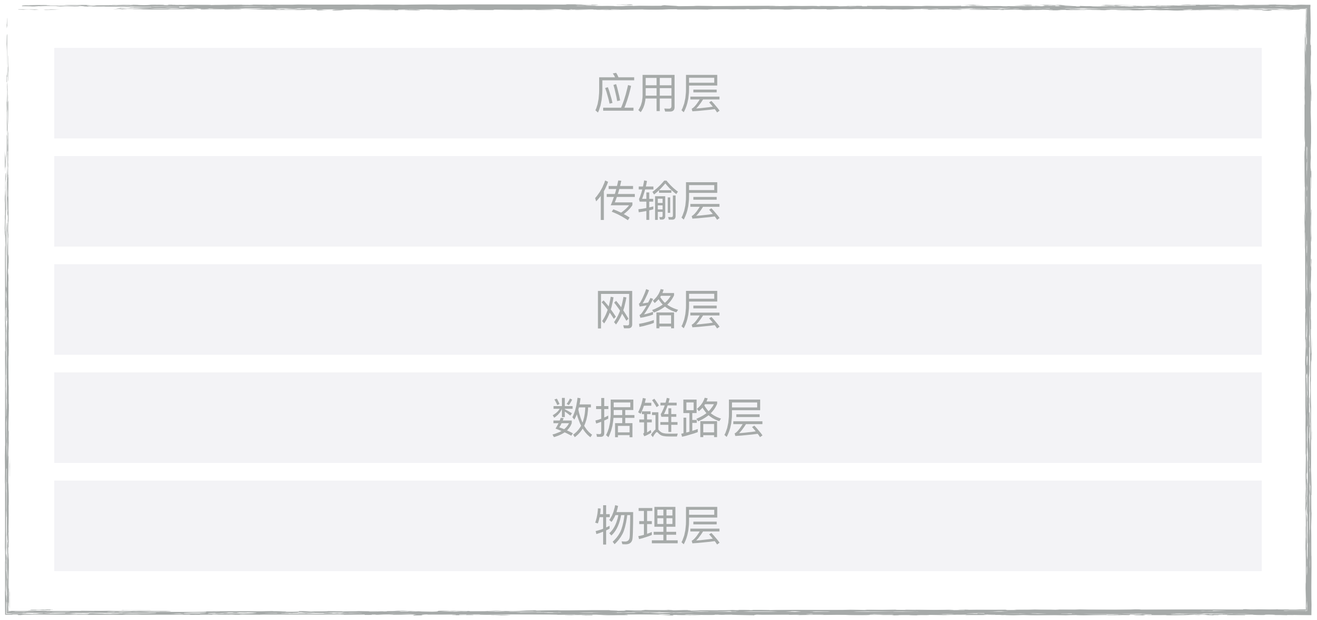
```
[root@cloud ~]# nmap 101.78.230.76 --scanflags SYN,FIN -p 80

Starting Nmap 5.51 ( http://nmap.org ) at 2014-06-03 17:43 CST
Nmap scan report for 101.78.230.76
Host is up.
PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.35 seconds
[root@cloud ~]#
```

```
[root@cloud ~]# tcpdump -i lo host 101.78.230.76 and port 80 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol dec
ode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
17:43:22.460898 IP 101.78.230.76.37201 > 101.78.230.76.80: Flags [FS],
seq 342802321, win 1024, options [mss 1460], length 0
17:43:23.462404 IP 101.78.230.76.37202 > 101.78.230.76.80: Flags [FS],
seq 342867856, win 3072, options [mss 1460], length 0
```

利用协议栈



[OUTLINE]

- 漏洞与利用
- 分工专业化
- 黑客

[分工专业化]

开发、运维；
漏洞的发现、利用，权限接入、维持。

分工专业化

[OUTLINE]

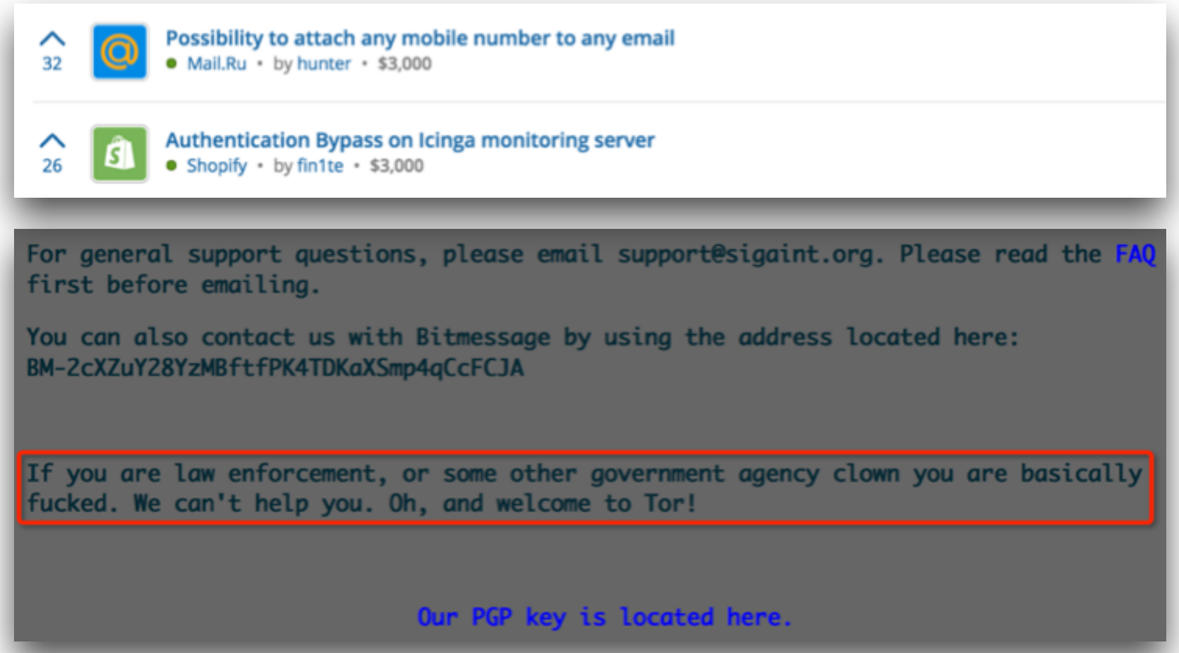
- 漏洞与利用
- 分工专业化
- 黑客

[黑客]

发现和利用这些代码疏漏的人。

发现/利用代码疏漏：

- 发现漏洞
- 利用漏洞
- 利用漏洞获取权限
- 利用漏洞保持权限并创造一个舒适的环境深入，并保持隐蔽和匿名



■匿名性
- 整体指导思想
- 了解自己所使用的技术栈
- 不要依赖单一信任点

■exploit的使用
- 私有exploit
- 公开exploit

■功能
- 减少对系统的更改

谢谢