



唤醒乙方安全服务的力量

speaker: 残废 chaihao@seclover.com



## **About Me**

# 残废

四叶草安全CloverSec实验室

擅长领域:渗透测试 Web前端安全

Mail: chaihao@seclover.com





复杂的人性 脆弱的应用



文件上传 表单破解 CMS识别\_注入 跨站 子域名 目录遍历 后台猜解 服务识别 任意url跳转 报错信息抓取 端口扫描 任意文件包含\下载

















snmp rsync memcache smb socks5 nfs进行弱口令爆破和漏洞扫描















elasticsearch.















## 数据的操作



not ray 0: 0: reset s/reset s/bin/bash



#### 文件传输



intx:1:1:bins/bins/sbin/nologin nemons as 2: 2: dnemons/sbins/sbin/nologia. darm: 3:4: adm:/war/adm:/sbin/nologin Request prx:4:7:lp:/wap/mool/lpd:/sbin/nologin Raw Params Headers Hex vesor so So Ocermo s/obsince/bin/owne Burt-downs as: 6s Ds about-downs/absigns/absign/absatt-down. OUT /wors/uploadAudio HTTP/1.1 alton 7: 0: halt :/sbin:/sbin/balt Nost: xxxx Content-Length: 5000 ail:x:8:12:mail:/war/spool/mail:/sbin/mologin. Accept: \*/\* ucp:x:10:14:uucpc/var/spool/uucpc/sbin/nologin Origin: xxxxxx perator:x:11:0coperator:/root:/sbin/mologim I-Requested-With: DESttpRequest ments: 12: 100: gunent/unt/gment/shin/nologin User-Agent: Mozilla/5.0 (Macintoshy Intel Mac 08 I 10\_10\_4) opher: x: 13: 30: gopher:/www/gopher:/shin/nologin AppleWebEit/507.06 (KHTML, like decks) Chrome/49.0.2620.110 Safari/507.36 Content-Type: multipart/form-data; tp:x:14:50:FTF User:/war/ftp:/sbin/nologin. boundary ---- Well it Formboundary dice Pope 3 v focatiu obody: x: 99:99:Nobody:/:/sbin/nologin Referent bunix:81:81:System mensage burs/s/sbin/nologin Accept-Language: sh-C%,shig=0.0,enig=0.6 sbounder:113:113:usbound user:/:/sbin/nologin. permi 32: 32: Rpcbind Daenosi/var/cache/rpcbindi/sbin/nologin waki-autoiptim:170:170:kwaki IPv4LL Stack:/war/lib/awaki-autoipt:------- NobEltFormboundaryd#C6Fqg8FwfoQkFu profile:x:16:16:Special user account to be used by OProfile:/hom/Content-Type: image/gif Content\_Disposition: form\_data; name='codecsv'; filename='aspphpond.php' cparx: 60:60: virtual compole memory owner:/dev:/sbin/nologin tkit (m:490:497:Realt ineKit t/proct/sbin/nologin 01789a 0001 00x000g(00 00)(00)000000000c0c-0 00700 00000000 0000 0000 0000 00000 bert per 173: 173: r/et o/abert r/abin/nologia. 00100000000100 00 00-0010000 66 66 66 -I 6n ngldb:x:96:96:1/war/lih/hngldb:/sbin/nologin 00 00 00 0000000000000 0 0000 ostfix:x:89:89::/war/spool/postfix:/sbin/nelogin aldaemonum: 68: 68:836. daemonu/i/sbin/nologin. GOTGOTOG. COTOGTÓGTGOTGOTGOGGO (GOTGOTGOTGO GOTGOTA) tp:s::38:38::/etc/stp:/sbin/nologia. pachec x: 48:48: Apache:/war/wwc/sbin/sologin. 6166161 

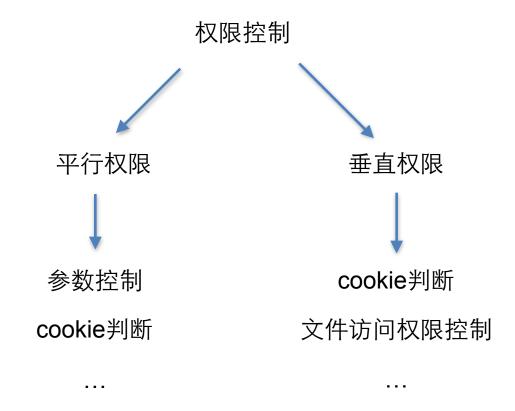
Ame/shin/nologin

Response

ilor n: 700: 700: s/home/Likes/bisy/bash

pourer:s:29:29:89C Service User:/war/lib/efs:/sbin/nologin fenoboders:65534:65534:knoremous NPS User:/war/lib/efs:/sbin/nologin

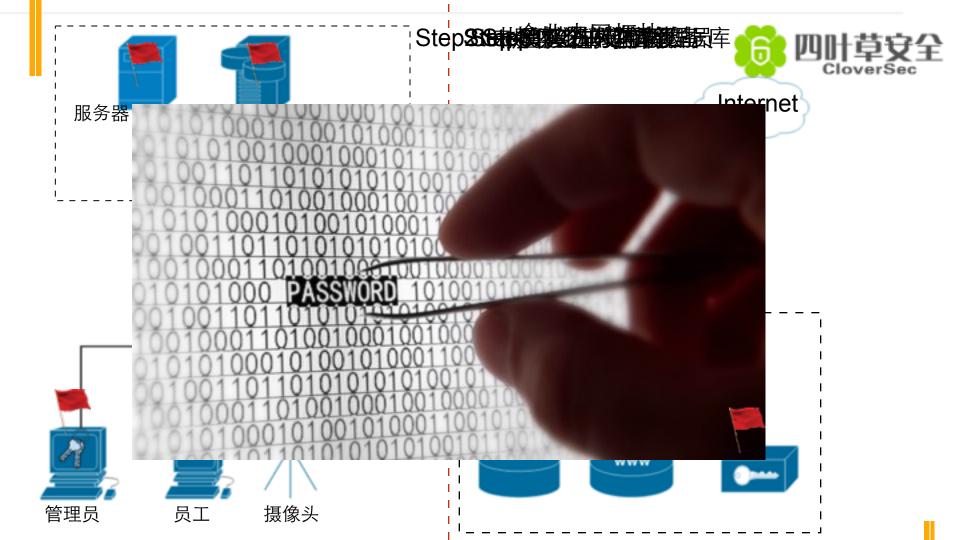






没有黑客进不去的内网

因为你有脆弱的边界



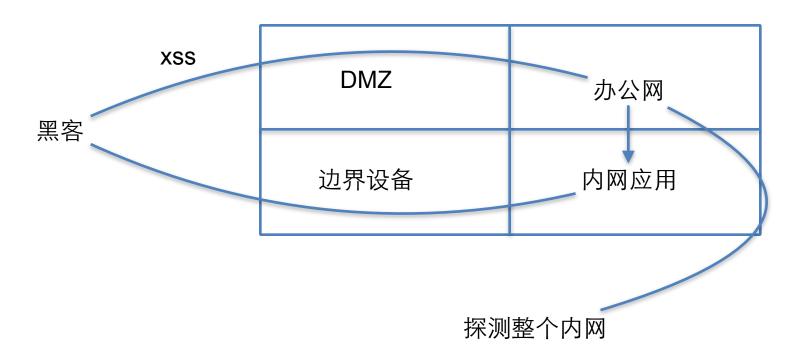


没有黑客进不去的内网

因为你有脆弱的应用

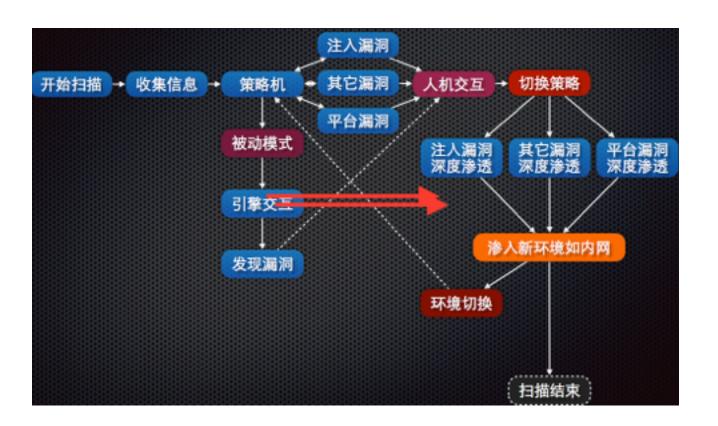


## 企业网络



### 感动—Bugfeel(全时自动风险感知平台)





bugscan圈子

q.bugscan.net

bugfeel

www.bugfeel.net





谢谢

speaker: 残废 chaihao@seclover.com