FREEBUF | 企业安全 俱乐部

乙方视角下的攻防演练实践

曾裕智

2019 | 企业安全俱乐部
数据治理专场

About me

曾裕智

漏洞盒子负责人

多年乙方安全服务经验

安全测试

攻防演练

应急演练的重要性

2013年，韩亚航空214航班着陆时发生事故。飞机尾部撞到了机场防波堤上，导致机尾整截脱落，飞机主体机身偏出跑道，起火燃烧。机组人员的镇定快速有效的指挥，机组+乘客307人，304人得救。民航空难史上的奇迹。

企业就像一架在空中高速飞行的客机

安全事故来临时，机组人员能否快速地应急处理，避免重大人员资产损失？

攻防演练背景

- 企业的安全防御是否有效？
- 安全设备策略是否会被绕过？
- 员工是否有足够的安全意识避开水坑攻击、钓鱼攻击？
- 攻击事件发生时，安全团队是否能及时发现？
- 能否在攻击成功前阻断其行为？
- 日志记录是否完备，事后溯源是否可快速定位问题？
- ……

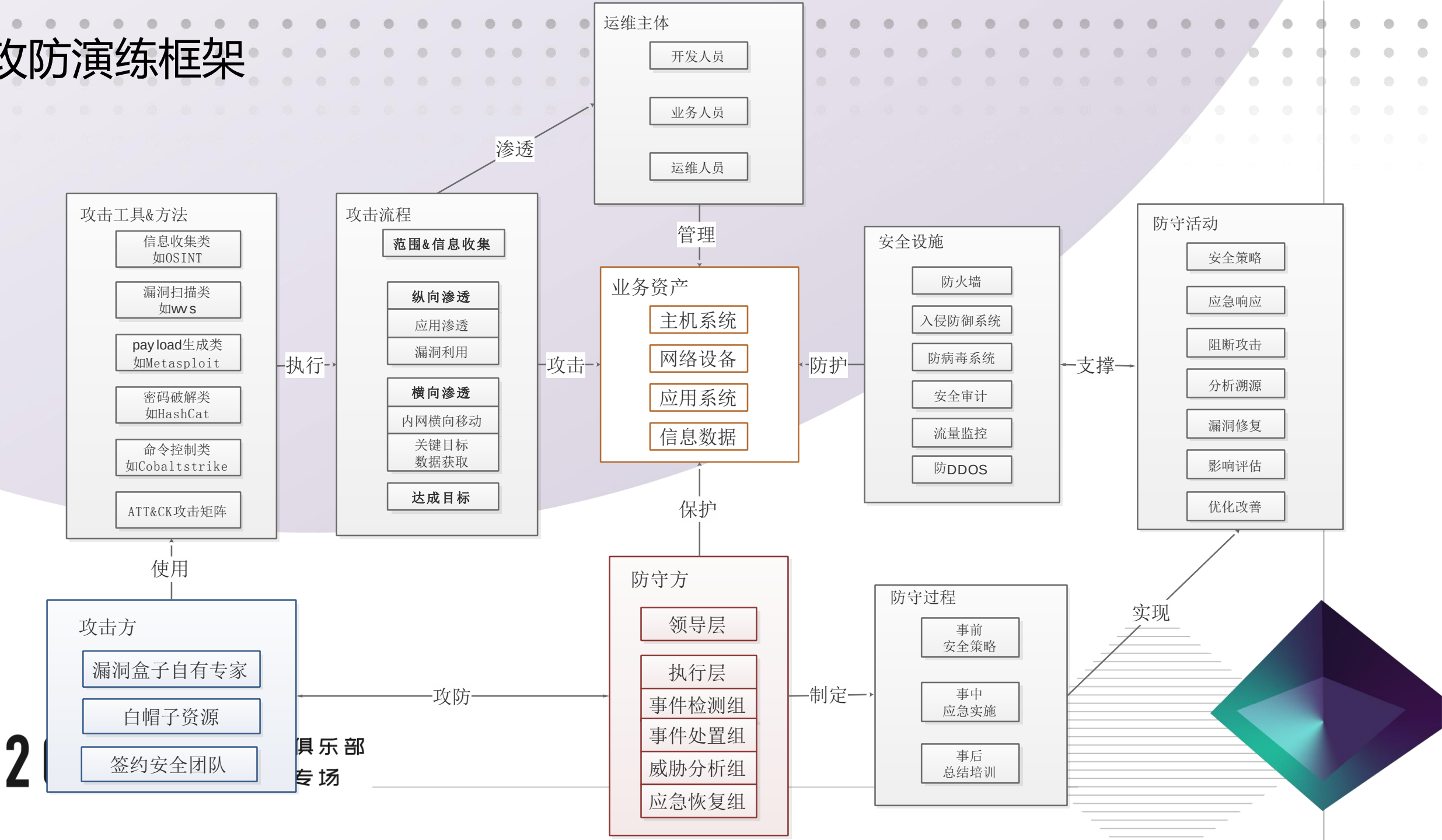
攻防演练目标

- 安全产品是否可以防护和检测到新的攻击手段，了解安全短板
- 安全防护体系是否有效的形成纵深防护，增加攻击者的消耗
- 内部人员是否具备相关安全意识，抵御外部攻击
- 安全管理中的协同是否可以有效的执行和响应，安全人员是否可以应对新形式下的安全威胁的响应

攻防演练与渗透测试区别

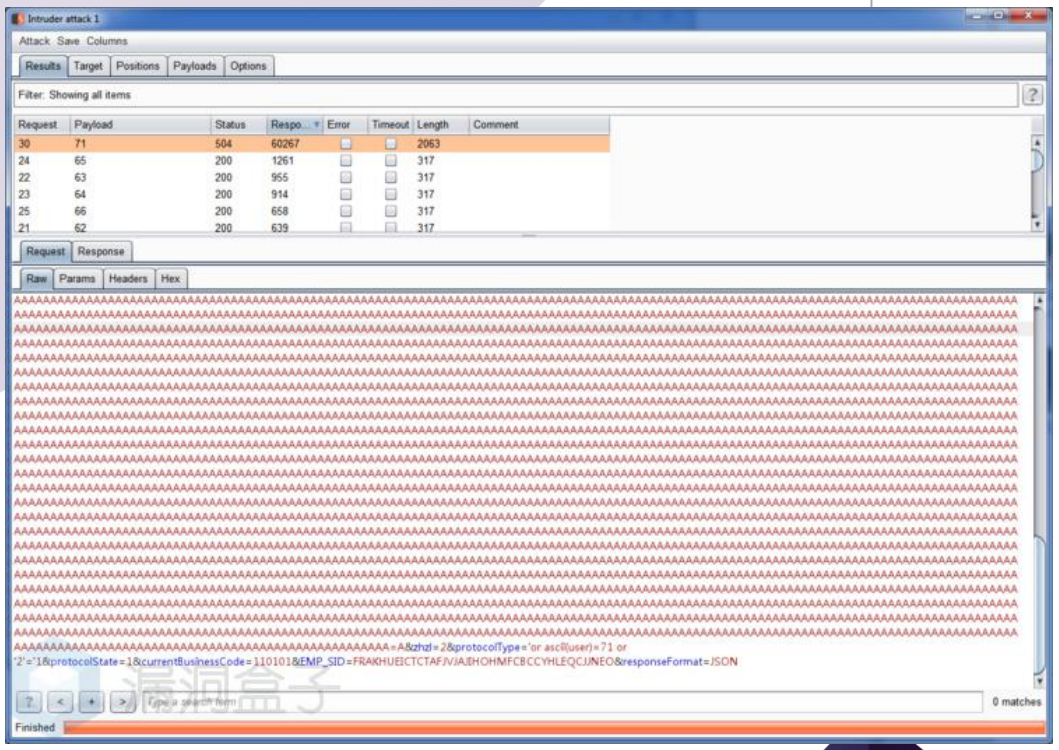
	攻防演练	安全/渗透测试
目的	目的不在发现漏洞多少而在于： 检验防御有效性； 检验应急处置能力； 检验人员安全意识；	尽可能多发现安全漏洞，测试面全覆盖。
实施方式	攻击方需要隐藏自身，绕开防御设备，深入横向渗透； 攻击方式除了系统漏洞本身，还有社工、钓鱼等； 漏洞需要评估对业务实际影响；	攻击方无需隐藏自身。漏洞点到为止。
参与对象	过程需双方参与，防守方需要积极防御，并做相应应急响应 。	过程中主要乙方参与，完成渗透并输出报告 。

攻防演练框架


运维主体
开发人员
业务人员
运维人员
渗透
管理
攻击工具&方法
信息收集类
如OSINT
漏洞扫描类
如wvs
payload生成类
如Metasploit
密码破解类
如HashCat
命令控制类
如Cobaltstrike
ATT&CK攻击矩阵
执行
攻击流程
范围&信息收集
纵向渗透
应用渗透
漏洞利用
横向渗透
内网横向移动
关键目标
数据获取
达成目标
攻击
业务资产
主机系统
网络设备
应用系统
信息数据
防护
安全设施
防火墙
入侵防御系统
防病毒系统
安全审计
流量监控
防DDOS
支撑
防守活动
安全策略
应急响应
阻断攻击
分析溯源
漏洞修复
影响评估
优化改善
使用
保护
实现
攻击方
漏洞盒子自有专家
白帽子资源
签约安全团队
攻防
防守方
领导层
执行层
事件检测组
事件处置组
威胁分析组
应急恢复组
制定
防守过程
事前
安全策略
事中
应急实施
事后
总结培训

攻防案例分享：WAF攻防

- 防守方：核心业务部署WAF防护，开启策略
- 攻击方：进行SQL注入，尝试绕过WAF检测
- 攻防结果：攻击方通过构造超长数据包，成功绕过WAF规则检测，并SQL注入获取数据库名。防守事中无法检测发现。
- 优化改善：升级WAF规则，调整策略。



攻防案例分享：WiFi劫持、钓鱼邮件

■ 攻击方：

1）现场通过伪造WiFi信号，尝试劫持企业普通员工数据；

2）远程发送钓鱼邮件，诱导企业员工点击。

■ 攻防结果：

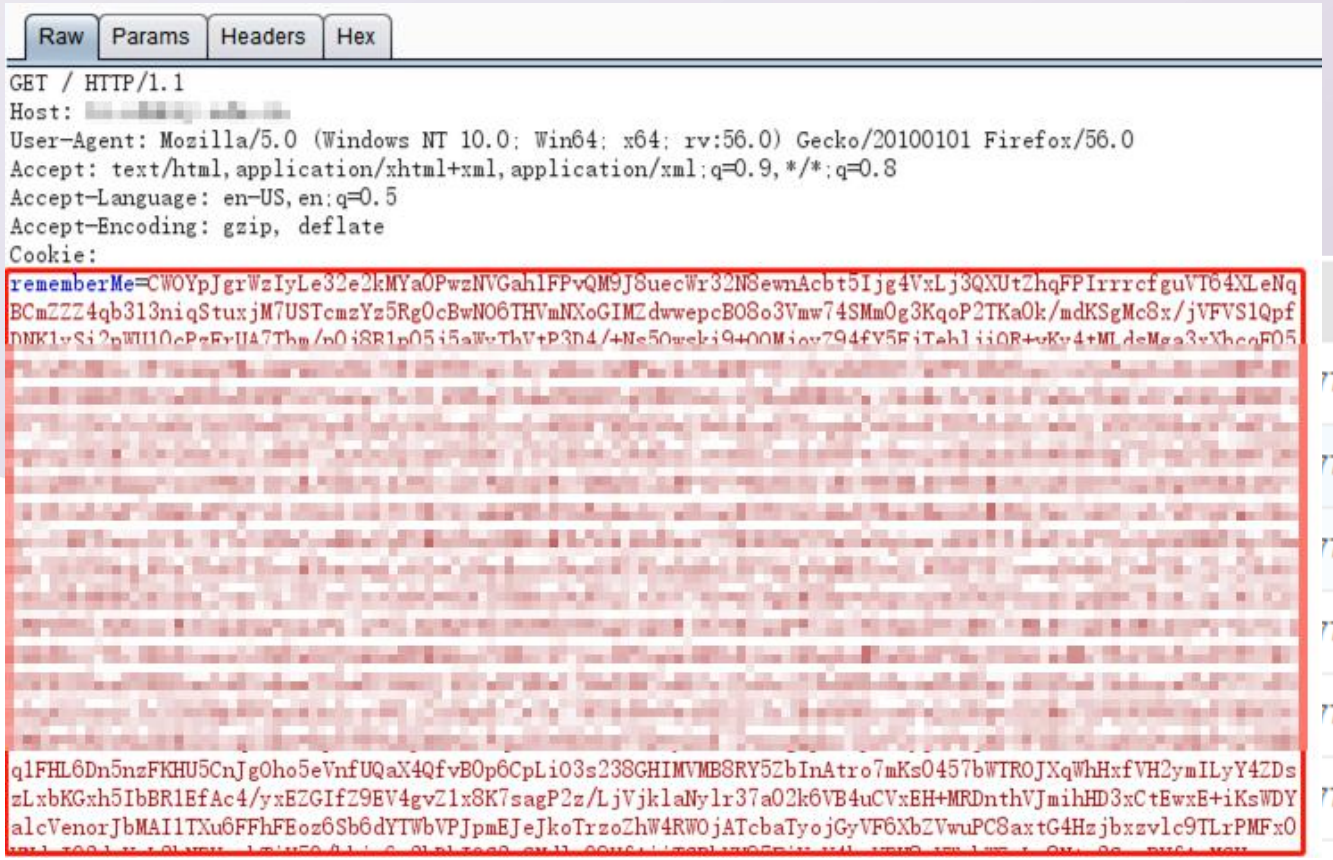
部分员工缺乏信息安全意识，连接名称相同或相似的WiFi，完全无感知地遭受中间人劫持攻击，泄露个人信息。甚至在个别案例中意外发现开发将项目代码上传到公网网盘。

■ 优化改善：

加强员工安全意识培训；企业邮箱配置SPF防止伪造等；

攻防案例：横向渗透

从企业公网子站shiro反序列化到拿下内网域控的横向渗透。



攻防案例：横向渗透

尝试使用powershell反弹，均失败，服务器有相关防护，无法直接启用。绕过手法为将powershell.exe复制到其他目录并改名，成功反弹shell：

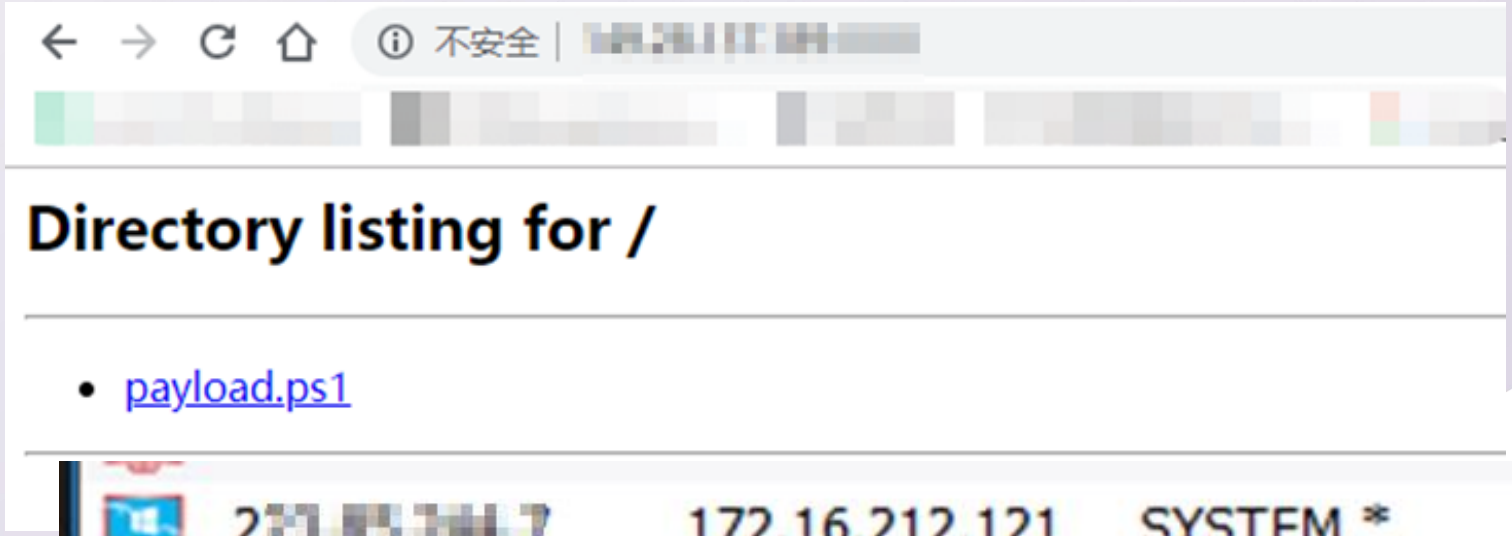
```
Listening on [0.0.0.0] (family 0, port 12345)
Connection from [                ] port 12345 [tcp/*] accepted (family 2, sport 54980)
Microsoft Windows [°汾 6.1.7600]
°  (c) 2009 Microsoft Corporationi£±£´ĘĘ{i£

E:\          \Tomcat7_mh>
```

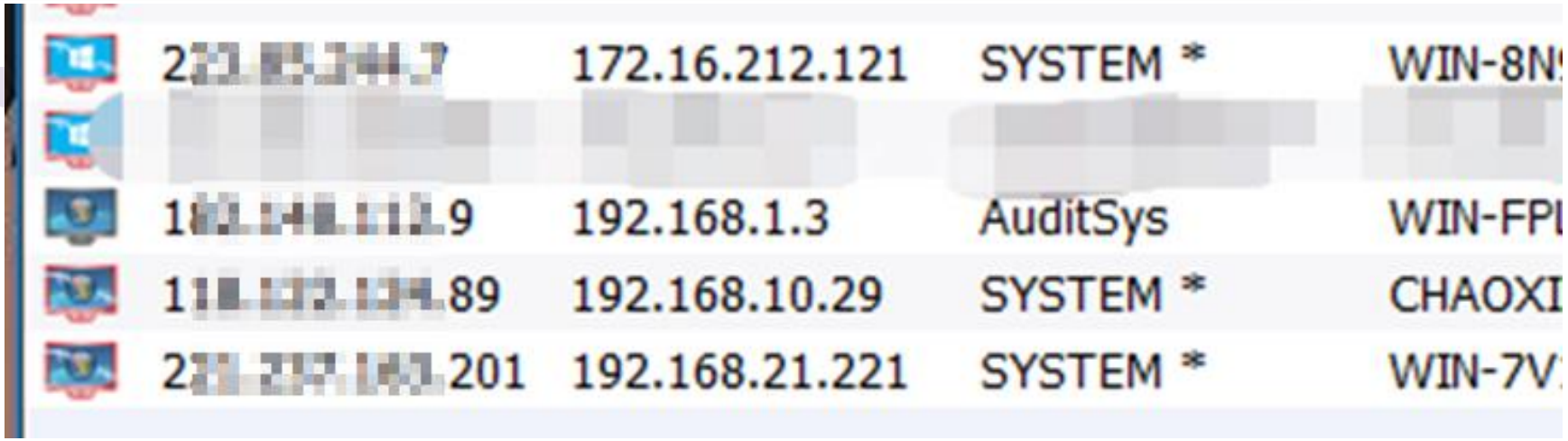
执行whoami，为system权限：

```
E:\          \Tomcat7_mh\webapps\ROOT>whoami
whoami
nt authority\system
```

攻防案例：横向渗透

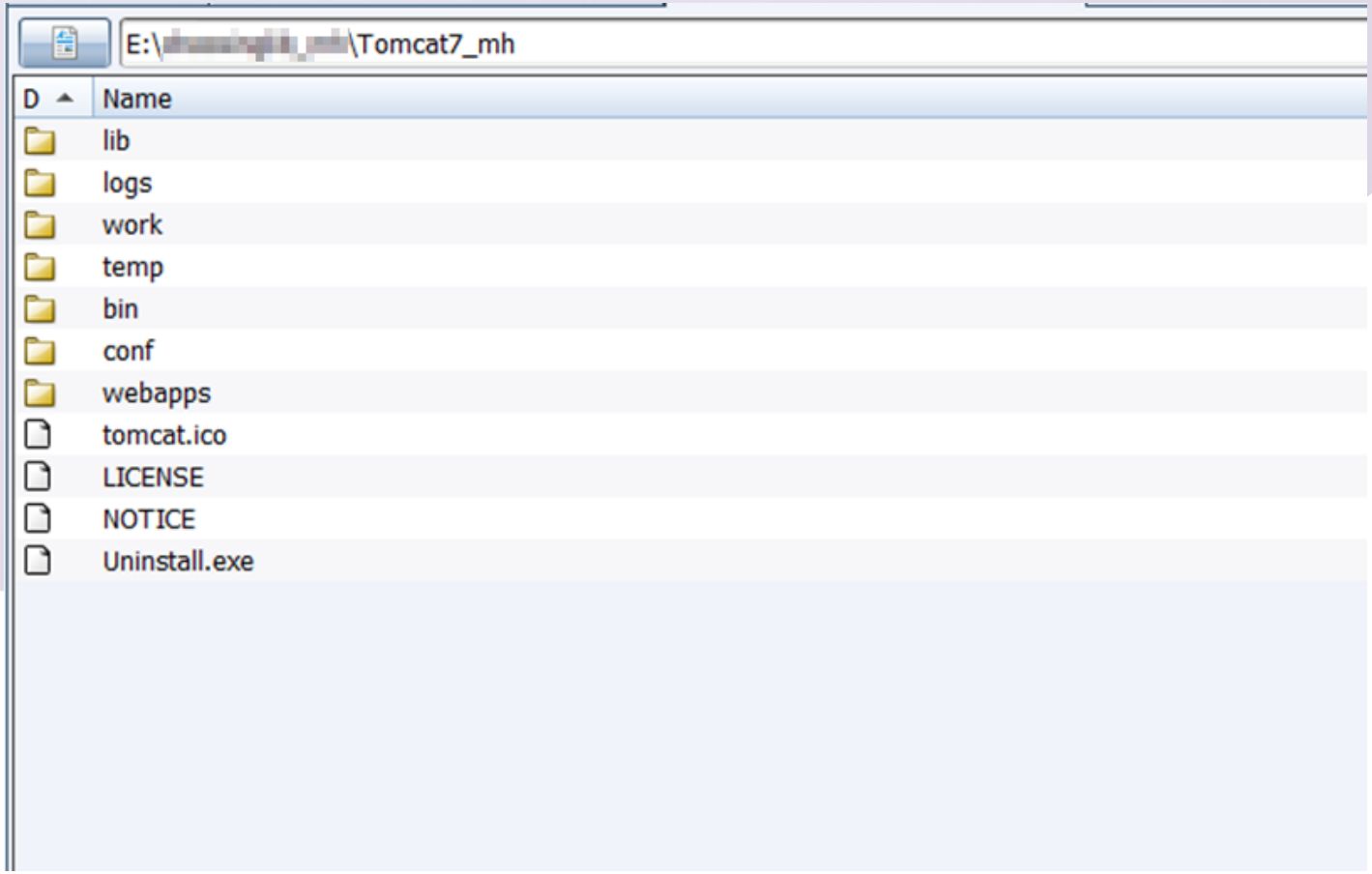
为方便进行内网渗透，采用cobalt strike 上线远控：





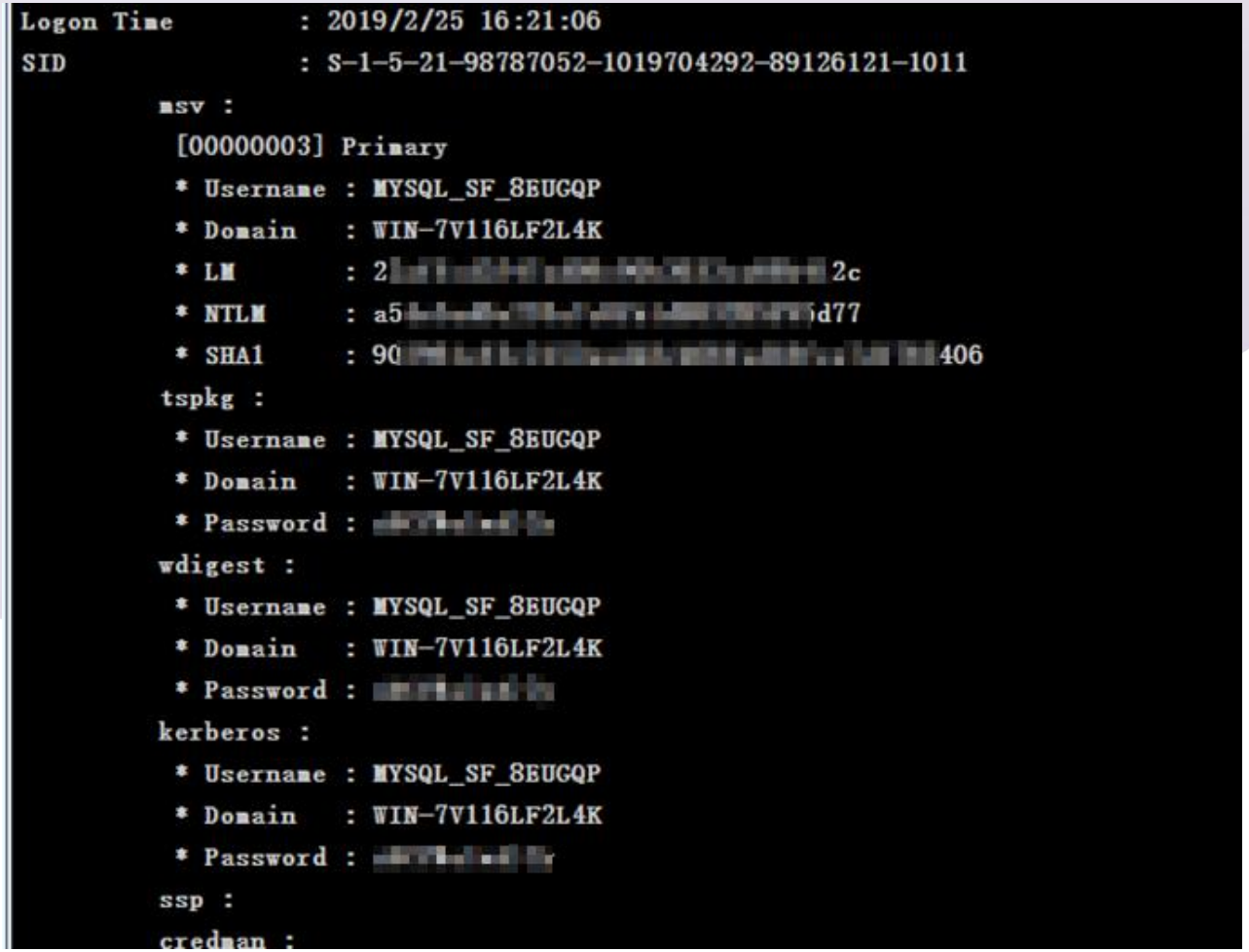
攻防案例：横向渗透

查看目录文件：



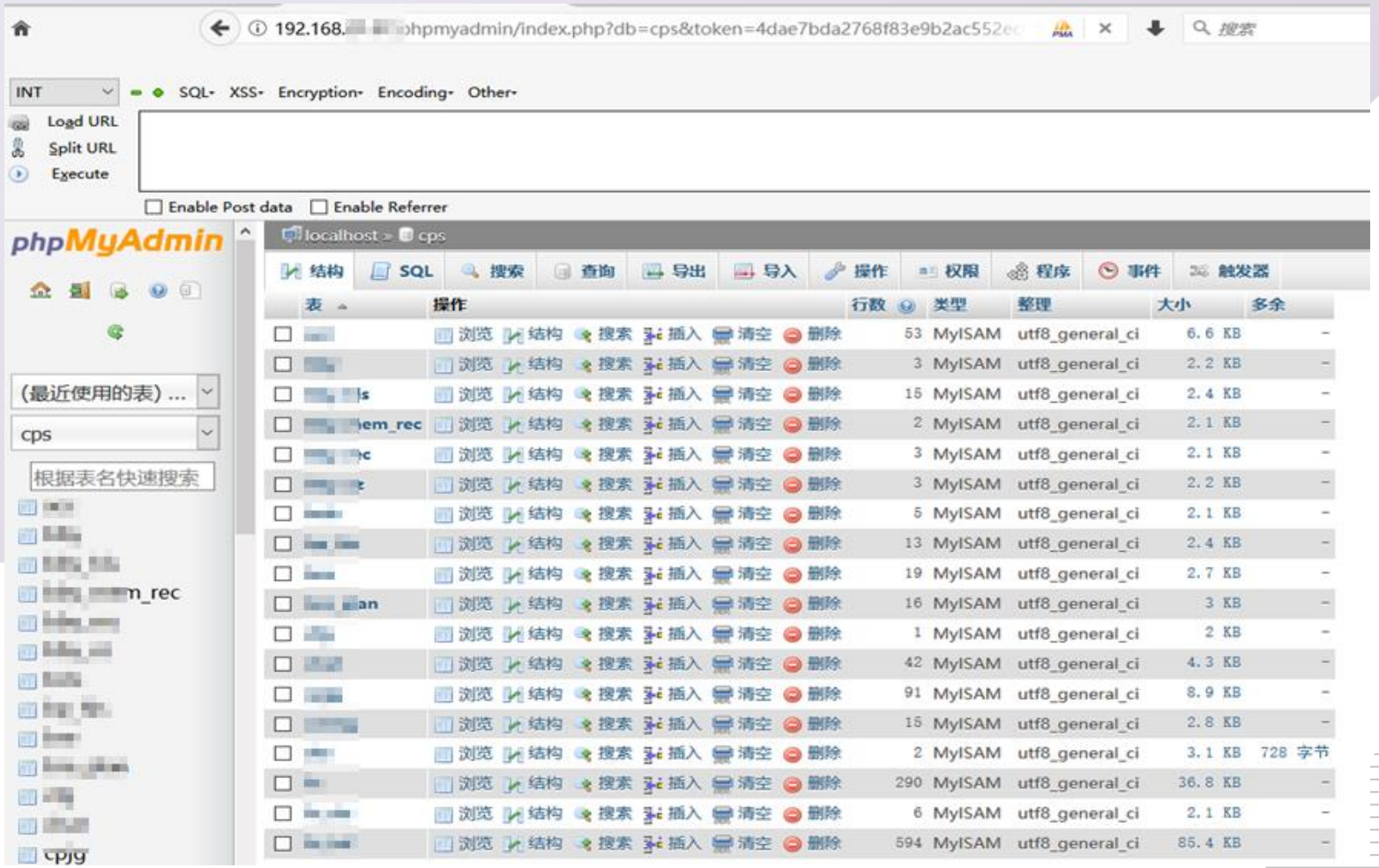
攻防案例：横向渗透

采用mimikatz成功读取内存中的密码：



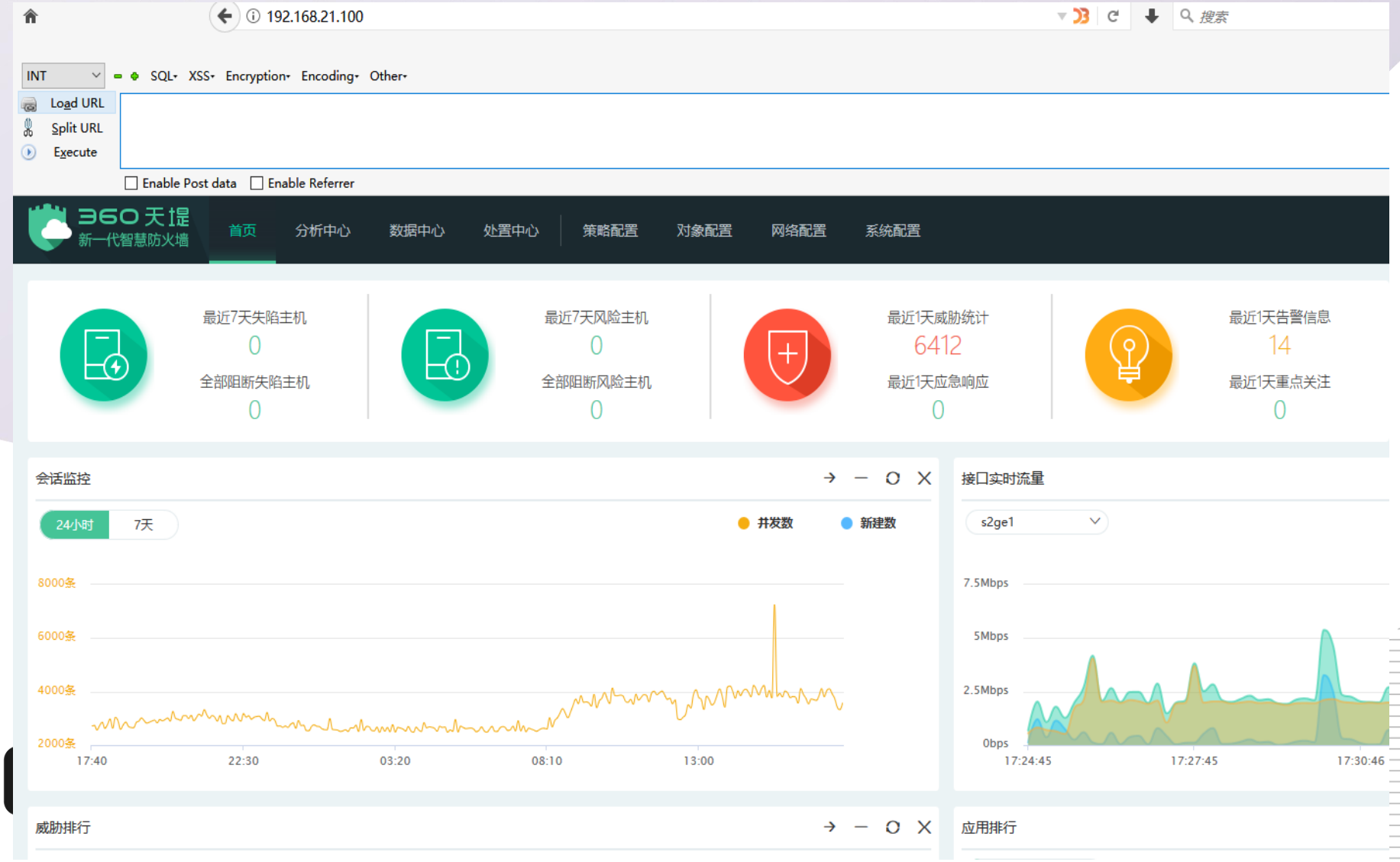
攻防案例：横向渗透

内网phpMyAdmin弱口令致数据库沦陷



攻防案例：横向渗透

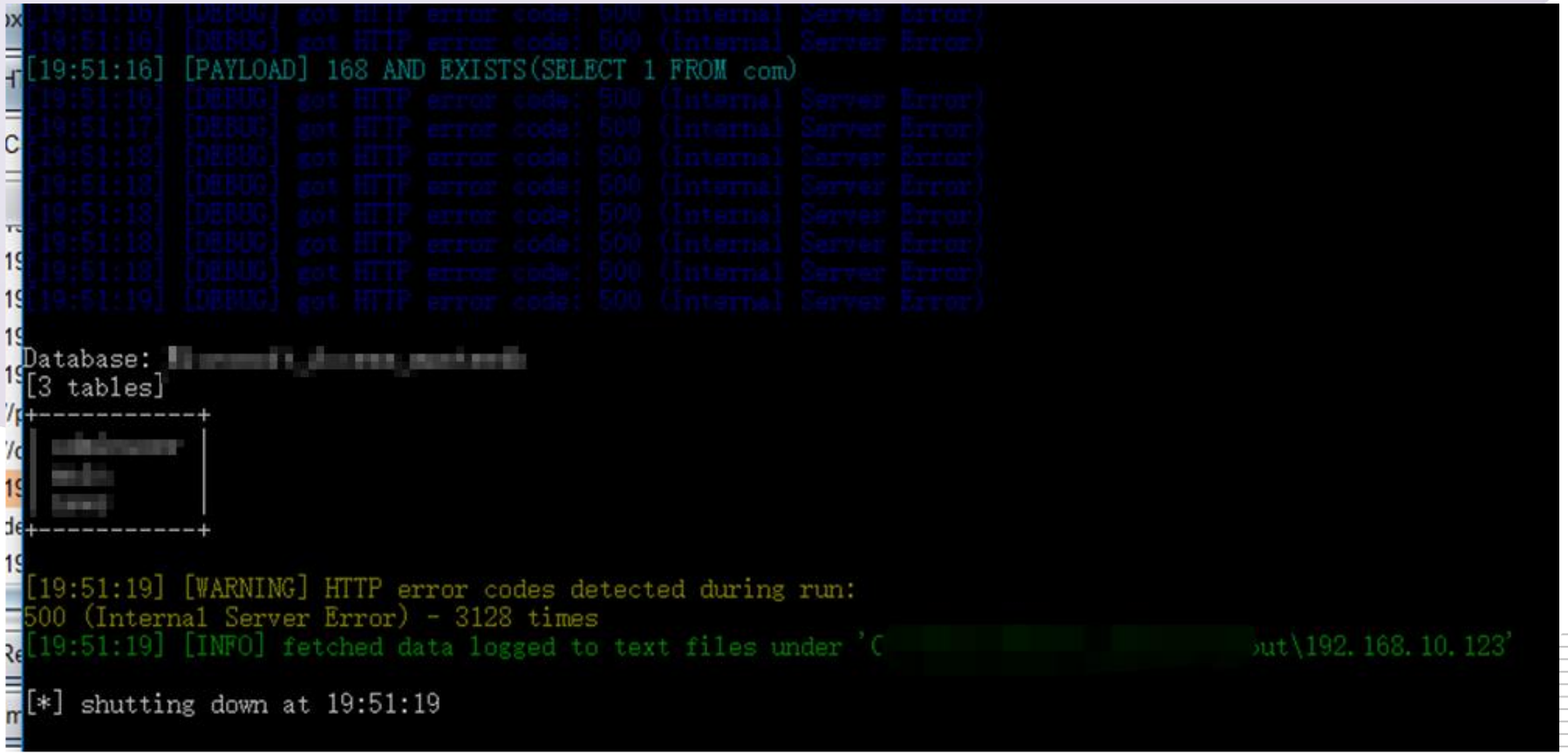
内网防火墙默认口令可监控内网所有流量



攻防案例：横向渗透

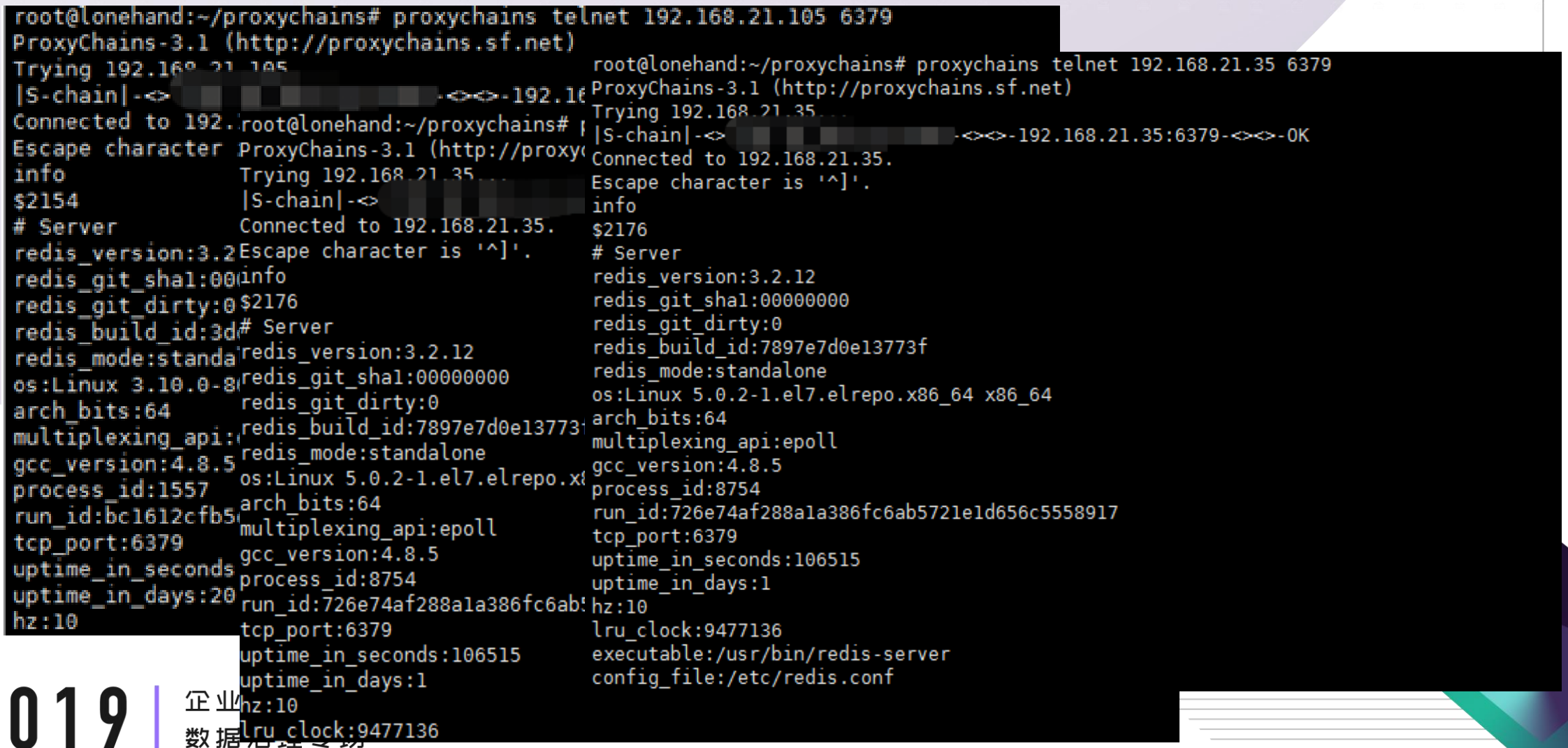
内网SQL注入致使内部数据库信息泄露

http://192.168.**.**/show_others.asp?id=266



攻防案例：横向渗透

建立Socks代理，开启内网扫描，发现大量Redis未授权访问：



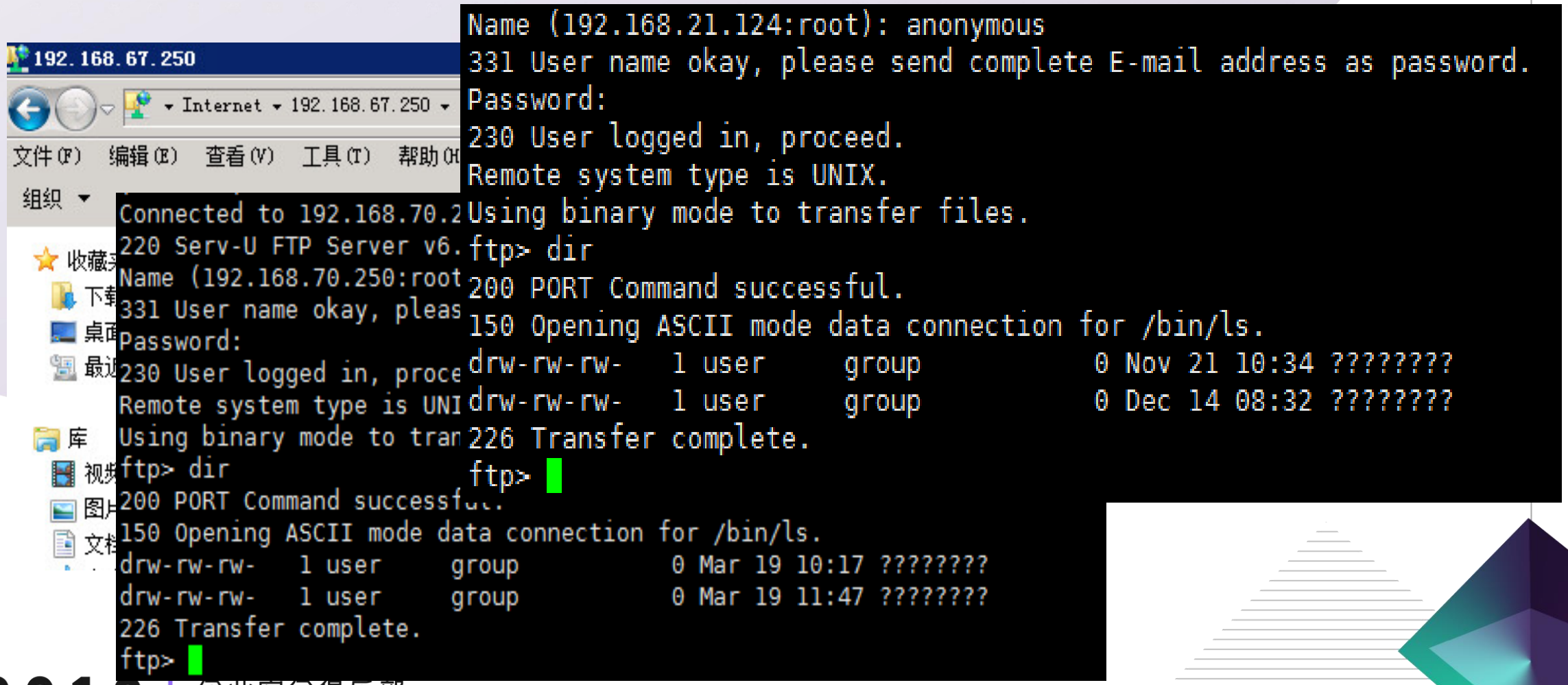
攻防案例：横向渗透

MongoDB未授权访问：

```
Host is up (0.0045s latency).
PORT      STATE SERVICE
27017/tcp open  unknown
| mongodb-info:
|   MongoDB Build info
|     ok = 1
|     debug = false
|     gitVersion = 1ef45a23a4c5e3480ac919b28afcba3c615488f2
|     sysInfo = Linux ip-10-67-194-123 2.6.32-220.el6.x86_64 #1 SMP Wed Nov 9 08:03:13 EST 2011 x86_64 BOOST_LIB_VERSION=1_49
|     loaderFlags =
|     maxBsonObjectSize = 16777216
|     OpenSSLVersion = OpenSSL 1.0.0-fips 29 Mar 2010
|     version = 3.0.6
|     bits = 64
|     javascriptEngine = V8
|     allocator = tcmalloc
|     compilerFlags = -Wnon-virtual-dtor -Woverloaded-virtual -std=c++11 -fPIC -fno-strict-aliasing -ggdb -pthread -Wall -Wsign-compare -Wno-
unknown-pragmas -Winvalid-pch -pipe -Werror -O3 -Wno-unused-local-typedefs -Wno-unused-function -Wno-deprecated-declarations -Wno-unused-but-
set-variable -Wno-missing-braces -fno-builtin-memcmp -std=c99
|     versionArray
|       1 = 0
|       0 = 3
|       3 = 0
|       2 = 6
|   Server status
```

攻防案例：横向渗透

FTP匿名访问/弱口令：



攻防案例：横向渗透

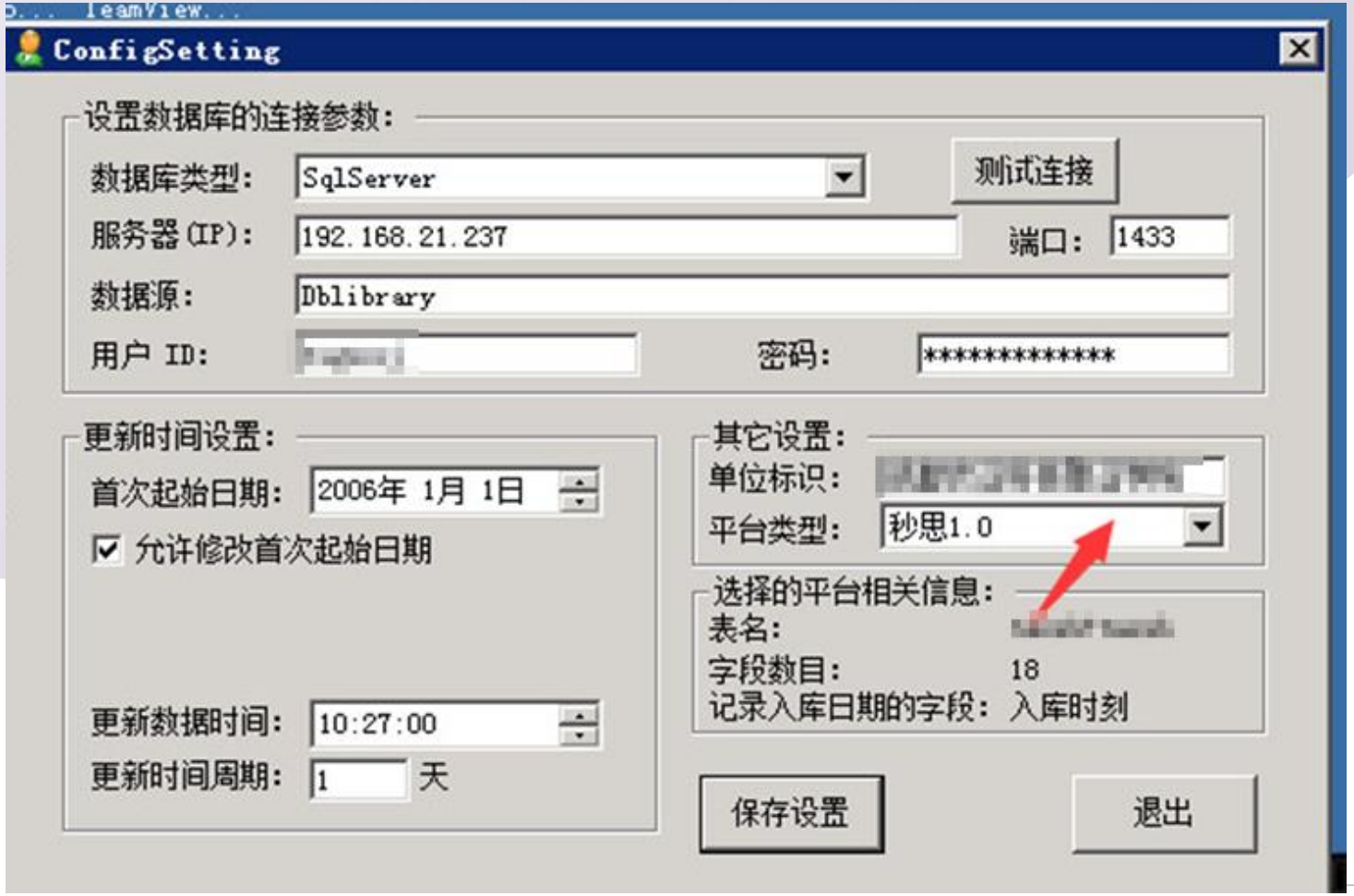
MySQL弱口令：

```
root@lonehand:~/proxychains# proxychains mysql -u root -p -h 192.168.21.8
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
|S-chain|-<>[redacted]<><>-192.168.21.8:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ;
Your MySQL connection id is 41
Server version: 5.1.41-community MySQL Community Se

Copyright (c) 2000, 2019, Oracle and/or its affili

Oracle is a registered trademark of Oracle Corporat
affiliates. Other names may be trademarks of their
owners.

Type 'help;' or '\h' for help. Type '\c' to clear t

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| [redacted]mation_schema |
| [redacted]         |
| [redacted]         |
| [redacted]         |
| [redacted]         |
+--------------------+
5 rows in set (1.37 sec)
```

```
root@lonehand:~/proxychains# proxychains mysql -u root -p -h 192.168.21.24
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
|S-chain|-<>[redacted]<><>-192.168.21.24:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 22
Server version: 5.6.24 MySQL Community Server (GPL)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| [redacted]mation_schema |
| [redacted]         |
| [redacted]         |
| [redacted]rmance_schema |
| [redacted]         |
+--------------------+
5 rows in set (1.49 sec)
```

攻防案例：横向渗透

SqlServer密码泄露：



攻防案例：横向渗透

意外之喜——连接内网一台SqlServer 服务器时，发现域管登陆过此台服务器，使用mimikatz读取密码，成功登录域控机器，至此成功获取域控权限。内网机器都在攻击者控制范围。

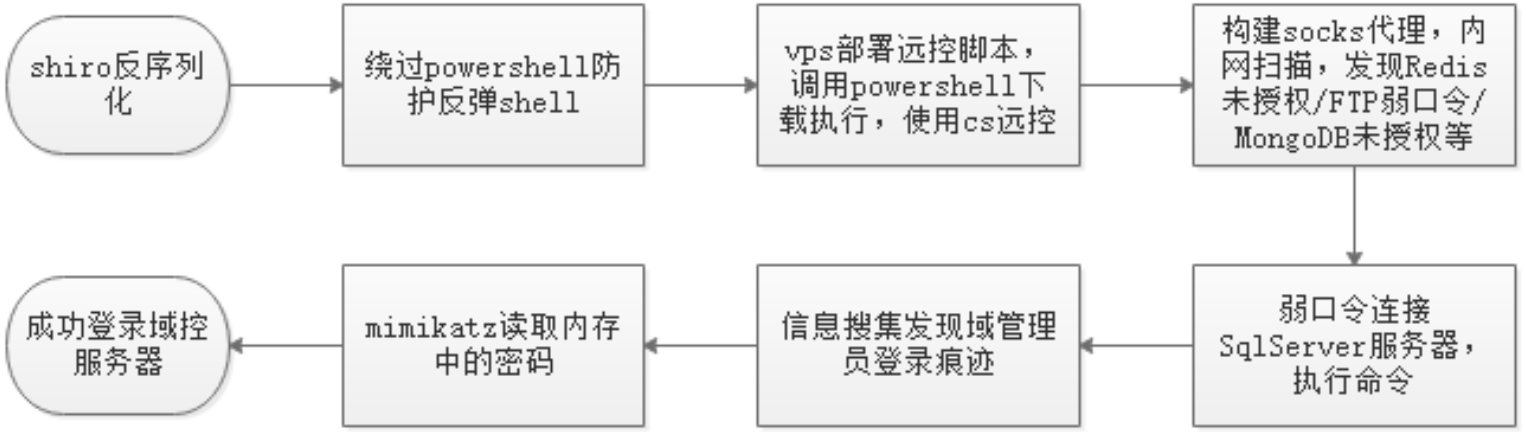
user	password	realm	note
Guest		172_27_0_12	
Administrator		172_27_0_12	
cdslndx_1		172_27_0_12	
administrator		CHAOXING-XUNDI	
Administrator		CHAOXING-XUNDI	
Administrator		CHAOXING-XUNDI	
Administrator		iZ5361vzl6w4gjZ	
Guest		USER-082RJS69UH	
suyan		USER-082RJS69UH	
Guest		USER-082RJS69UH	
Administrator		USER-082RJS69UH	
Guest		USER-082RJS69UH	
MYSQL_SF_8EUGQP		WIN-7V116LF2L4K	
MYSQL_SF_8EUGQP		WIN-7V116LF2L4K	
MSSQL_SF_4Q721N		WIN-7V116LF2L4K	
tqzx-web		WIN-7V116LF2L4K	
tqzx-web		WIN-7V116LF2L4K	
MSSQL_SF_4Q721N		WIN-7V116LF2L4K	
Administrator		WIN-8N9418L9F88	

攻防案例：横向渗透

防守方暴露出的问题：

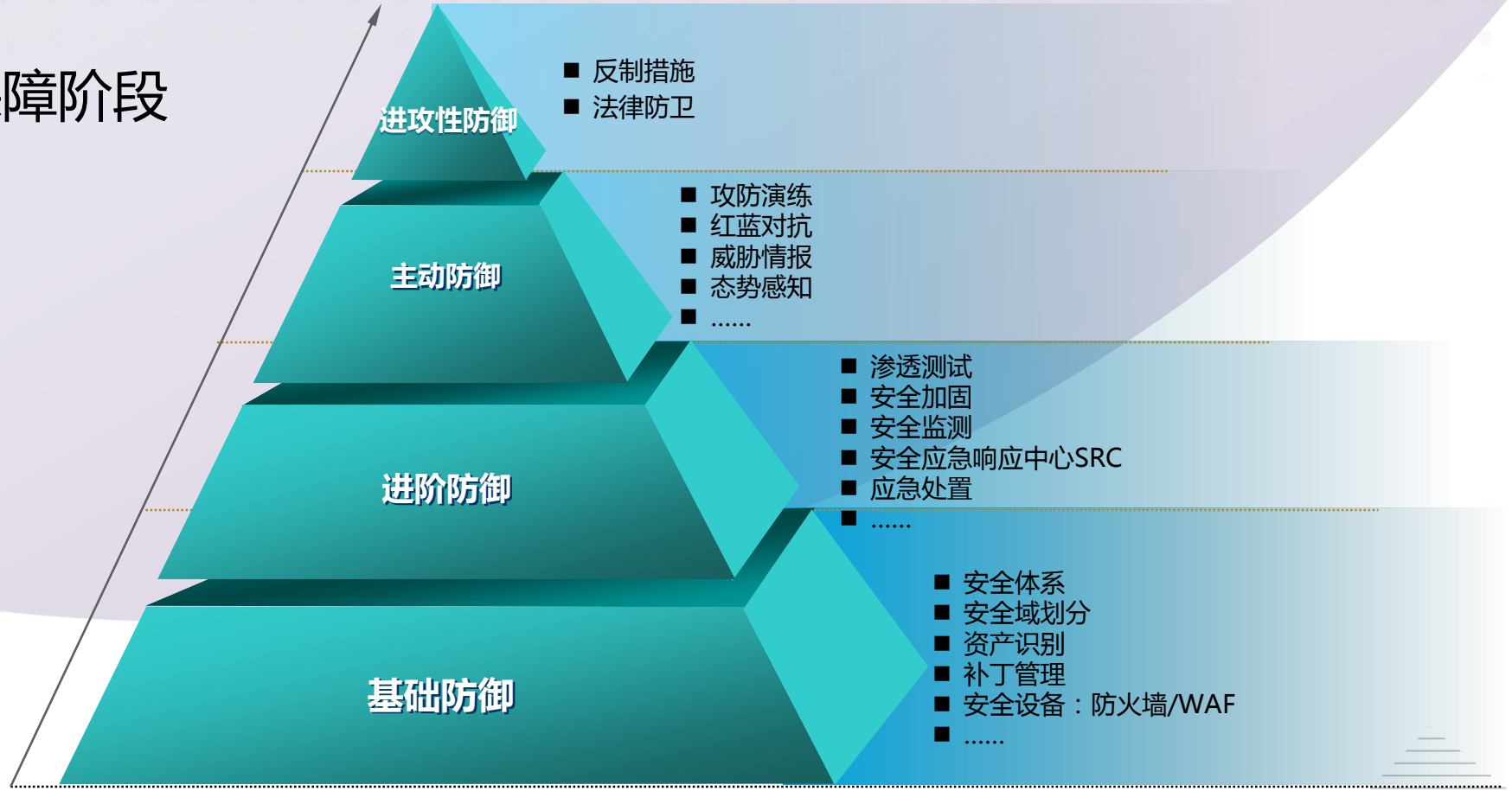
- 公网站点组件已知高危漏洞没有被及时修复整改
- 服务端缺乏恶意代码防范
- 安全设备使用默认密码
- 内网应用缺乏基本的安全访问控制
- 操作系统没有及时更新补丁
- 弱口令，内部人员缺乏安全意识
- ……

攻击路径回顾



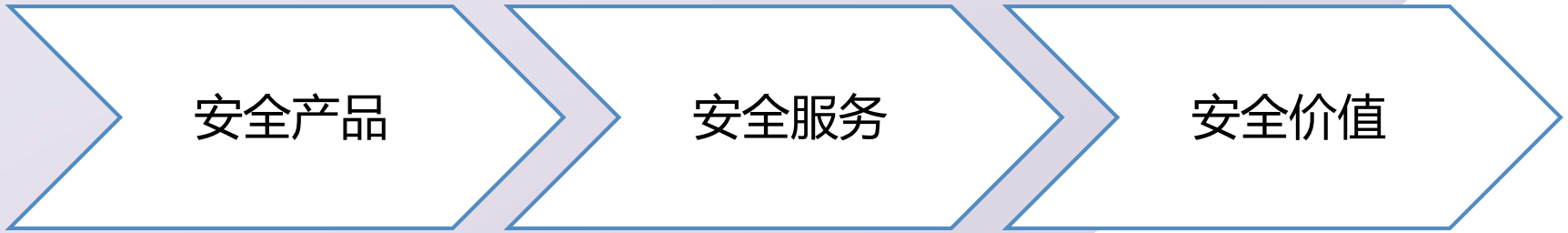
总结

安全进阶保障阶段


进攻性防御
反制措施
法律防卫
主动防御
攻防演练
红蓝对抗
威胁情报
态势感知
.....
进阶防御
渗透测试
安全加固
安全监测
安全应急响应中心SRC
应急处置
.....
基础防御
安全体系
安全域划分
资产识别
补丁管理
安全设备：防火墙/WAF
.....

总结

安全交付进阶：



攻防演练：安全价值交付的探索

THANKS

2019 | 企业安全俱乐部
数据治理专场